iBSolution

認証検疫アプライアンス

iBAQS

取扱説明書

目次

はじめに....4
本書の見かた....5
内容物に関して....5
著作権について....6
ご利用の前に....7
本書の構成....8
iBAQS について....9
動作環境について....12
各部の名称と働き....14
対応するネットワーク機器....16
システム構成について....17
環境条件....18
iBAQS のご利用手順....19
準備....20
iBAQS インストール....21
ﾎﾟﾘｼｰﾏﾈｰｼﾞｬｻｰﾊﾞの設定....21
ライセンスキー登録....22
各部の名称と機能....25
全体構成....25
ヘッダ....25
メニュー....26
メイン....27
監視....28
トップ....29
MAC 収集状況....33
不正アクセス状況....34
サービス状態....36
ネットワーク機器状態....38
通信制限状況....39
クライアント状態....40
ログ監視....43
認証ログ....45
AVS 確認ログ....47
管理ログ....49
設定....51
サーバ設定....53
冗長化設定....56
システム設定....58
ライセンス設定....62
外部連携設定....64
UPS 連携設定....65
SNMP マネージャ連携設定....66
管理者設定....68
証明書設定....70
認証局編集....72
クライアント証明書発行....74
クライアント証明書ﾀﾞｳﾝﾛｰﾄﾞ....76
DHCP 設定....78
セグメント追加....80
セグメント編集....82
セグメント削除....84
クライアント設定....85
クライアント追加....87
クライアント一括変更....90
クライアント一括削除....95
クライアント編集....96
クライアント削除....99
ネットワーク機器設定....101
ネットワーク機器追加....103
ネットワーク機器編集....105
ネットワーク機器削除....107
スケジュール設定....108
バックアップ設定....111
リストア....114
アップデート....116

管理. 118
ハードウェア状態. 119
通信確認. 121
ログアウト. 122
セカンダリ. 123
セカンダリ. 124
セカンダリ トップ. 124
セカンダリ サービス状態. . . . 126
その他. 128
ネットワーク機器の設定. 129
困ったときは. 135

はじめに

本書の見かた.....5
内容物に関して.....5
著作権について.....6

本書の見かた

本説明書ではご注意いいただきたい内容や参照ページを次のように記載しています。

メモ	知っておくと便利なことや、関連知識などを記載しています。
ご注意	操作上お守りいただきたい事項や、ご注意いただきたい事項を記載しています。
▸P. 00	参照するページを記載しています。

内容物に関して

ご使用の前に、次のものがそろっているかご確認ください。万一、不足しているものがあった場合は、お買い上げの販売店にお問い合わせください。

●iBAQS 本体（アプライアンス製品）
1U のラックマウント型サーバです。
ラックマウントキット取り付け済。

●iBAQS ライセンス証書
本製品のライセンスキーを記載しています。

●iBAQS ドキュメント CD
本製品のドキュメントが収録されています。

●電源ケーブル
3P の AC ケーブルです。
AC 100V 専用です。

●梱包物一覧
梱包物の一覧が記載されています。

著作権について

権利者の許諾を得ることなく、このソフトウェアおよび取扱説明書の内容の全部または一部を複写すること、およびこのソフトウェアを賃貸に使用することは、著作権法上禁止されています。

ソフトウェアを使用したことによるお客様の損害、または第三者からのいかなる請求についても、アイビーソリューション株式会社は一切その責任を追いかねます。このソフトウェアの仕様は、改良のため予告なく変更する場合がありますが、ご了承ください。

Microsoft、Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

その他、本書で登場するシステム名、製品名は、一般に各開発メーカーの登録商標あるいは商標です。

ご利用の前に

本書の構成.....8
iBAQS について.....9
動作環境について.....12
各部の名称と働き.....14
対応するネットワーク機器.....16
システム構成について.....17
環境条件.....18
iBAQS のご利用手順.....19

本書の構成

本書の構成は次の通りです。

■ご利用の前に

iBAQS の特長や動作環境など、あらかじめ知っておいていただきたいことについて説明します。

■準備

ライセンスキーの登録など、iBAQS の準備内容を説明します。

■監視

各種ステータス、ログの内容について説明します。

■設定

iBAQS の各種設定方法について説明します。

■管理

管理に利用できるツールついて説明します。

■セカンダリ

冗長構成時のセカンダリ機について説明します。

■その他

エラーメッセージの見かたやシステム異常時の対処方法について説明します。

iBAQS について

iBAQS は認証スイッチと連携した不正アクセス防止機能、アンチウイルスソフト（以降 AVS と表記）の動作を確認し、ネットワークへの接続を制御する検疫機能を提供します。ネットワークプリンタやインテリジェントスイッチ等、AVS を導入できない機器では MAC ベース認証機能のみの利用もできます。また、DHCP サーバや各種アラートメール通知機能を備え、iBAQS 上でクライアント、認証スイッチの一元管理を行うことができます。

本製品は以下の特長があります。

●MAC アドレス収集モード

MAC ベース認証で通知される MAC アドレスを収集します。MAC アドレス収集モードが有効な場合、クライアントの通信が認証スイッチで阻害されることはありません。

●認証 DHCP サーバ

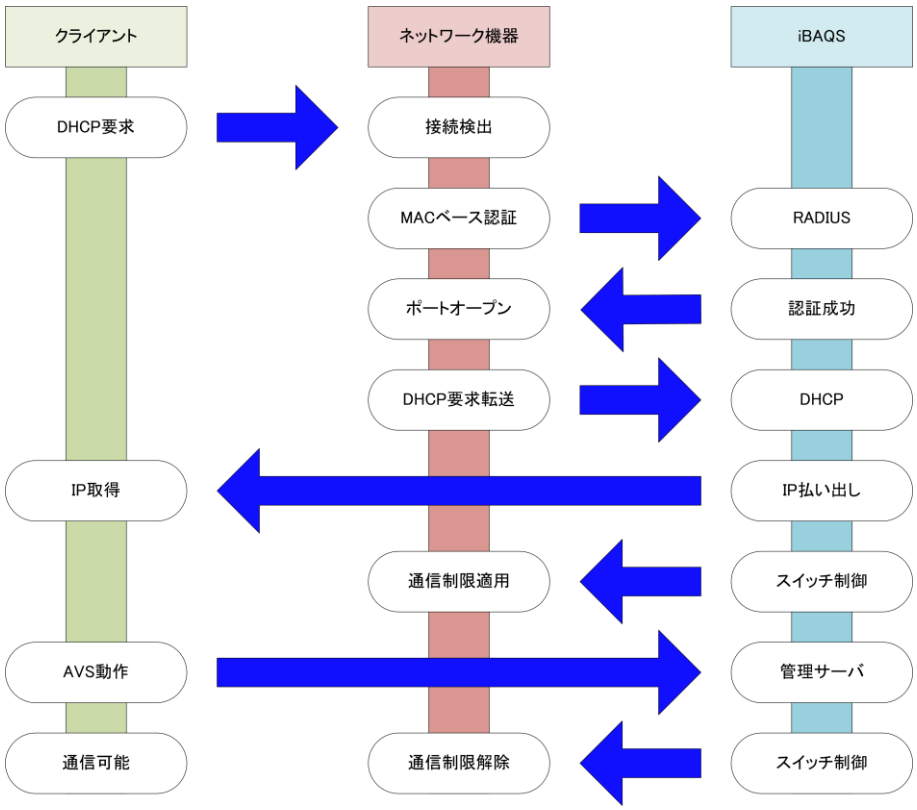
iBAQS は未登録クライアントからの DHCP 要求に対して IP アドレスを払い出しません。不正クライアントが非認証ポートに接続しても IP アドレスが取得できずネットワークに接続することはできません。

●エージェントレスの検疫機能

クライアントはエフセキュア アンチウイルス ワークステーションまたはエフセキュア クライアント セキュリティを導入して管理サーバとして iBAQS を指定するだけです。クライアント起動時に認証、AVS 確認が行われ、ログイン時には検疫が完了しています。(MAC ベース認証、EAP-TLS 使用時)

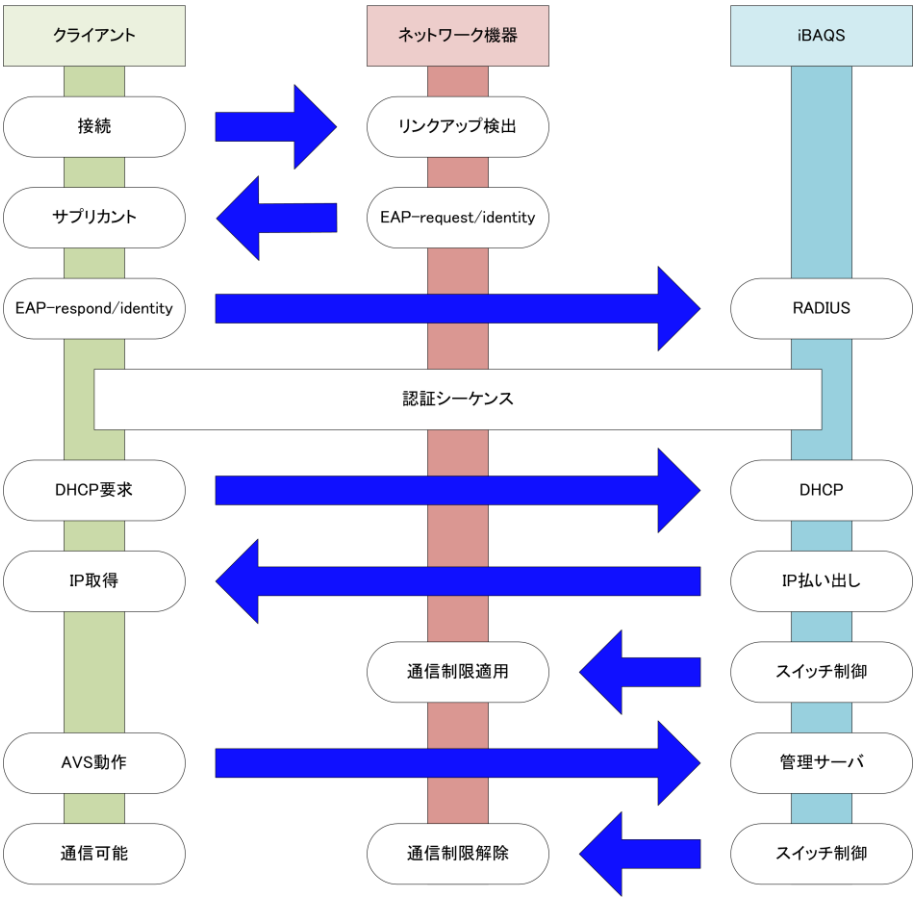
認証検疫動作概要(MAC ベース認証の場合)

クライアントが送信する DHCP 要求をトリガーにネットワーク機器はクライアントの MAC アドレスを用いた認証要求を iBAQS に出します。iBAQS が認証成功を応答するとクライアントはネットワークに接続できるようになり、先ほどの DHCP 要求は iBAQS に送られます。認証成功を検出すると同時に iBAQS はネットワーク機器を制御し、通信制限を適用、クライアントが iBAQS 以外のホストと通信できない状態にします。クライアントは IP アドレスを取得し、AVS が動作していることを管理サーバに伝えます。iBAQS は管理サーバから AVS の動作を確認するとスイッチに適用している通信制限を解除します。
※固定 IP での運用は推奨しません。クライアントが固定 IP の場合には DHCP 要求の代わりに Gratuitous ARP が MAC ベース認証のトリガーとなります。固定 IP で運用する場合も DHCP で運用する場合と同様に iBAQS にクライアントの登録が必要です。



認証検疫動作概要(IEEE 802.1X 認証の場合)

クライアントがネットワーク機器に接続すると IEEE 802.1X 認証が開始します。認証シーケンスが成功するとクライアントはネットワークに接続できるようになり DHCP 要求を送信します。iBAQS はネットワーク機器に認証成功を検出すると同時に iBAQS はネットワーク機器を制御し、通信制限を適用、クライアントが iBAQS 以外のホストと通信できない状態にします。クライアントは IP アドレスを取得し、AVS が動作していることを管理サーバに伝えます。iBAQS は管理サーバから AVS の動作を確認するとスイッチに適用している通信制限を解除します。



動作環境について

本製品を使うには、以下のハードウェアが必要です。各ハードウェアの取扱説明書をお読みのうえ、環境を確認してください。

サーバ環境（ソフトウェア版）

ハードウェア要件	- CPU：Pentium 4 2GHz 以上（3GHz 以上を推奨） - メモリ：512MB 以上（1GB 以上を推奨） - HDD：80GB 以上（160GB 以上を推奨） - ネットワーク：RJ-45（100BASE-TX）×1 以上 冗長構成時は GbE×2 を推奨 - 台数：1 台以上（2 台を推奨） ※冗長構成でご利用頂くには 2 台分のライセンスが必要です。

サーバ環境（アプライアンス版）

ハードウェア仕様	- CPU：Intel Atom D510 - メモリ：1GB - HDD:160GB - ネットワーク：RJ-45×2（GbE） - USB：USB 2.0×2 - 形状：ラックマウント（1U） - 外形寸法：437(W)×249(D)×43(H)mm - 重量：4.5kg - 最大消費電力：60W

サーバ環境（共通）

OS	専用 Linux
その他	インターネットへの接続環境（パターンファイル更新のために必須）

クライアント環境（検疫対象）

パソコン	- CPU：600 MHz 以上（1GHz 以上を推奨） - メモリ：256MB 以上（512MB 以上を推奨） ※Vista では 512MB 以上（1GB 以上を推奨）
OS	Microsoft® Windows® XP(32bit のみ,SP3 以降) Microsoft® Windows® Vista(32bit,64bit) Microsoft® Windows® 7(32bit,64bit) Microsoft® Windows® 8(32bit,64bit)
ソフトウェア	エフセキュア クライアントセキュリティ エフセキュア アンチウイルス ワークステーション
その他	IEEE 802.1X 認証を利用する場合には Windows®標準搭載のサプリカントが利用可能（ログオン前認証を併用することを推奨）

●Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標です。

クライアント環境（認証のみ）

クライアント	制限なし
OS	制限なし
その他	IEEE 802.1X 認証を利用する場合にはサプリカントが必要

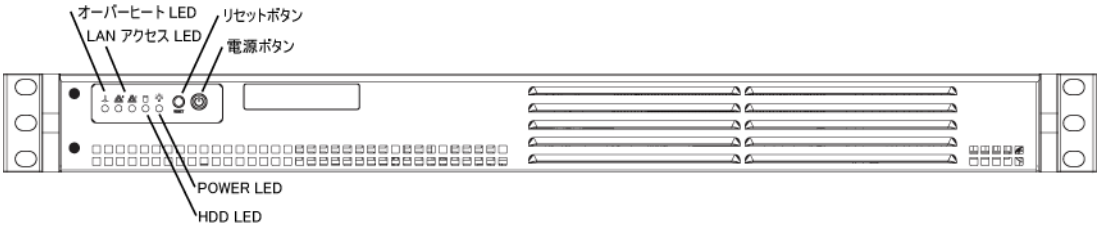
ブラウザ環境

クライアント	Microsoft® Windows® XP Microsoft® Windows® Vista Microsoft® Windows® 7 Microsoft® Windows® 8
ブラウザ	Internet Explorer 6 Service Pack 1 以降 Mozilla Firefox 3.5 以降

各部の名称と働き

アプライアンス製品の各部の名称とその働きは以下の通りです。

前面



(1)オーバーヒート LED

オーバーヒート状態にあるときに点灯します。点灯した場合には周囲のエアフローを確認してください。

(2)LAN アクセス LED

ネットワークリンク時に点灯、アクセス時に点滅します。

(3)HDD LED

内蔵ハードディスクドライブのアクセス時に点灯します。

(4)POWER LED

本機の通電状態を表示します。

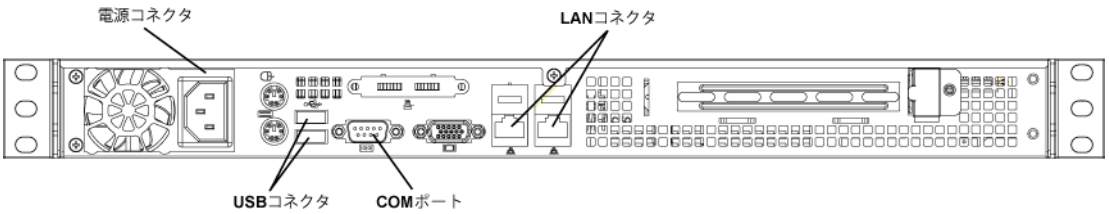
(5)リセットボタン

押すとリセットを実行します。通常は使用しないでください。

(6)電源ボタン

電源を ON/OFF するスイッチです。一度押すと POWER ランプが点灯して ON の状態になります。4 秒以上押し続けると強制的に電源を切ることができます。通常はウェブの管理画面から電源を切ってください。

背面



(1)電源コネクタ

AC コードを接続するコネクタです。

(2)USB コネクタ

USB インターフェースに対応している機器と接続します。

※本機では APC 社製 UPS との接続をサポートします。

(3) COM ポート

シリアルインターフェースを持つ装置と接続です。

※本機では使用しません

(4)LAN コネクタ

1000BASE-T/100BASE-TX/10BASE-T と接続するコネクタ

※向かって左が eth0、右が eth1 となります。

対応するネットワーク機器

本製品に対応するネットワーク機器は次の通りです。

※2013 年 8 月 現在

製造元	機種名
アライドテレシス	SwitchBlade x908、AT-x900-24XT、AT-x900-24XS AT-x900-12XT/S、CentreCOM 9924Ts、CentreCOM 9924T/4SP CentreCOM 9924SP、CentreCOM 8948XL、 AT-x610-48Ts/X-POE+(※注)、AT-x610-24Ts/X-POE+(※注) AT-x610-24SPs/X(※注)、AT-x610-48Ts/X(※注) AT-x610-24Ts/X(※注)、AT-x600-48Ts(※注) AT-x600-48Ts/XP(※注)、AT-x600-24Ts(※注) AT-x600-24Ts/XP(※注)、AT-x510-52GTX(※注) AT-x510-28GTX(※注)、AT-x510-52GPX(※注) AT-x510-28GPX(※注)、AT-x200-GE-28T(※注) AT-x200-GE-52T(※注)、AT-x210-24GT(※注) AT-x210-16GT(※注)、AT-x210-9GT(※注) CentreCOM 9424Ts/XP-E、CentreCOM 9424T/SP-E CentreCOM 8748SL、CentreCOM 8724SL、CentreCOM 8624EL CentreCOM 8624PS、CentreCOM 9424T/SP、CentreCOM 9408LC/SP CentreCOM 8424XL、CentreCOM 8424TX、CentreCOM 8324XL CentreCOM 8316XL

●SwitchBlade、CentreCOM はアライドテレシスホールディングス株式会社の登録商標です。

[メモ]

本製品は上記ネットワーク機器の各種類別に利用する機能を使い分けています。

ご利用される前にネットワーク機器の設定内容をご確認ください。

※【スイッチの設定】参照 （▶P. 129）

また、最新の対応するネットワーク機器の情報は、ホームページをご確認下さい。

[ご注意]

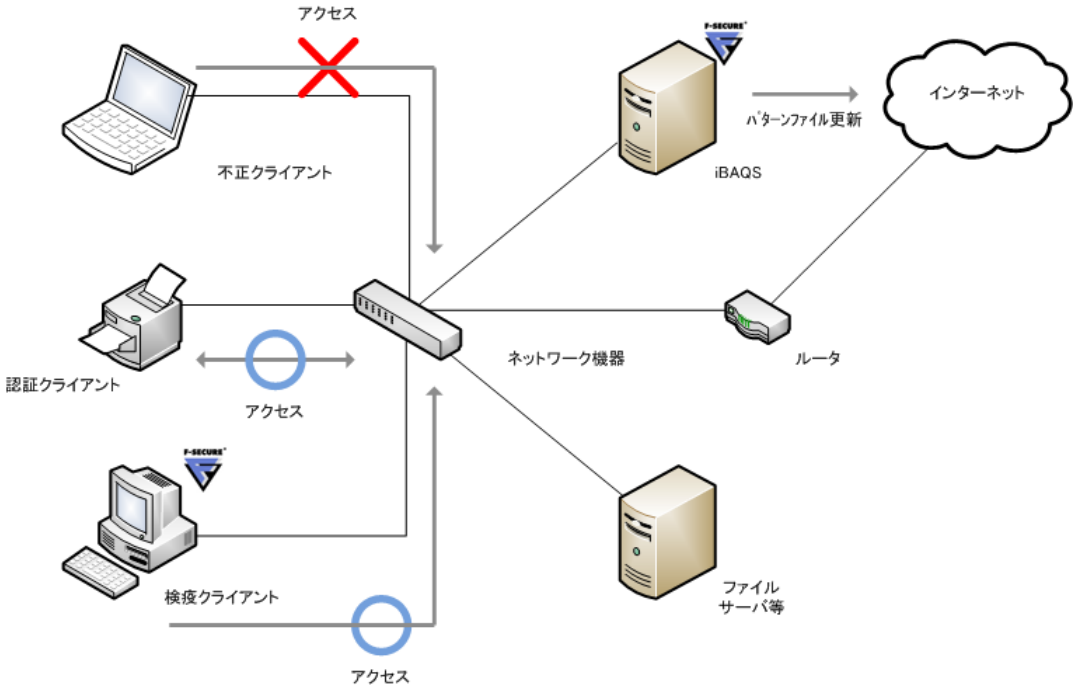
ネットワーク機器のハードウェアパケットフィルターには設定数の上限があります。設定数の上限を超えるクライアントを配下に接続しないでください。

詳細は、ネットワーク機器付属の取扱説明書を参照ください。

x610/x600/x510/x200/x210 シリーズでポートトランキングやスタック(VCS)を使用している場合、アクセス制限の設定、解除に時間を要する場合があります。ご了承ください。

システム構成について

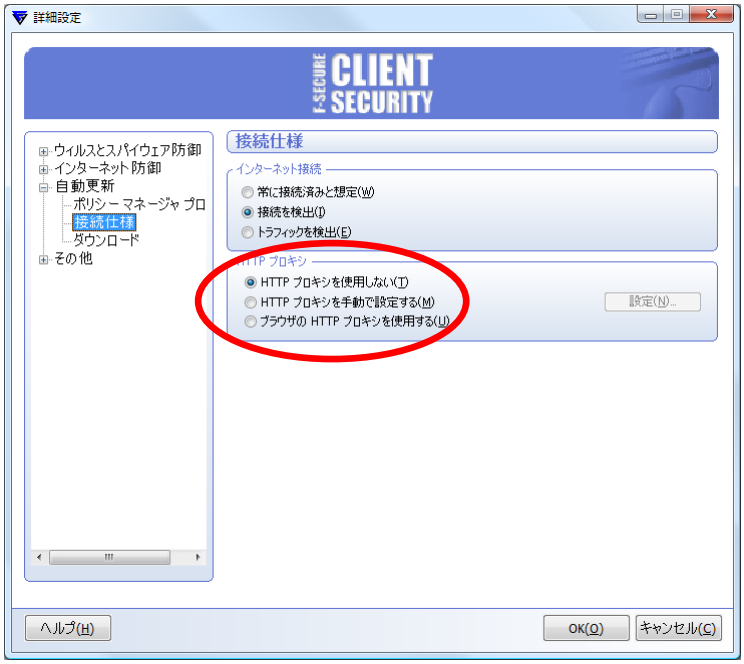
本製品を利用する際のシステム構成は次のようになります。



環境条件

本製品を導入する際の環境条件は次の通りです。

- クライアント(検疫対象)にエフセキュア アンチウイルス ワークステーションか エフセキュア クライアントセキュリティをインストールしてください。
- クライアント(検疫対象)の IP アドレスは、自動取得(DHCP)に設定してください。（※固定 IP アドレス環境は推奨しません。）
- クライアント(検疫対象)のアンチウイルスソフトウェアがブラウザに設定した プロキシ設定を利用しないように設定してください。エフセキュア・アンチウイルス導入手順書や下記設定例を参考にブラウザのプロキシを参照しないように設定してください。



- インターネットに接続可能な環境に設置してください。（パターンファイル更新、ライセンス有効期限取得のため）
- ネットワーク機器の死活確認に ping、制御に telnet を使用します。通信を阻害しないように設定を行ってください。ping の応答がない場合、機器の制御が行えません。

iBAQS のご利用手順

iBAQS のご利用手順は次の通りです。

STEP1	**システム環境を整える** ➢ iBAQS をインストールします。（ソフトウェア版のみ） ➢ iBAQS を設置します。 ➢ 対応するネットワーク機器を設置します。（▶ P.16）

↓

STEP2	**ライセンスキーを登録する** ライセンスキーを登録します。 ライセンス有効期限を取得するにはインターネットへの接続が必要です。

↓

STEP3	**各種設定を行う** ➢ iBAQS にネットワーク機器を登録します。 ➢ iBAQS にセグメントを登録します。 ➢ iBAQS にクライアントを登録します。 ➢ ネットワーク機器の設定を行います。 ➢ クライアントにエフセキュア社のアンチウイルス製品をインストールします。

↓

STEP4	**動作を確認する** 登録したクライアントが正しく認証、検疫できることを確認します。 アラートメールの設定を行った場合には

準備

iBAQS インストール. 21
ﾎﾟﾘｼｰﾏﾈｰｼﾞｬｻｰﾊﾞ 設定. 21
ライセンスキー登録. 22
各部の名称と機能. 25
全体構成. 25
ヘッダ. 25
メニュー. 26
メイン. 27

iBAQS インストール

ソフトウェア版は別紙 iBAQS インストール手順書に従ってインストールを行ってください。

[メモ]

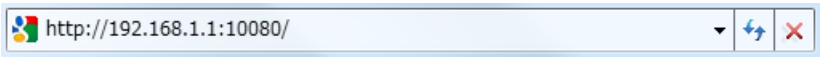
アプライアンス版では不要です。

ﾎﾟﾘｼｰﾏﾈｰｼﾞｬｻｰﾊﾞ設定

内蔵しているエフセキュア ポリシーマネージャサーバの管理者パスワードを設定します。

① **iBAQS と設定用のパソコンを同じスイッチ(ハブ)に接続し、iBAQS の電源を入れます**

② **ブラウザを使用して http://192.168.1.1:10080/または http://[インストール時に設定した IP アドレス]:10080/を開きます**



③ **管理者 ID でログインします**

[メモ]

初期の管理者 ID は【manager】、管理者パスワードは【friend】です

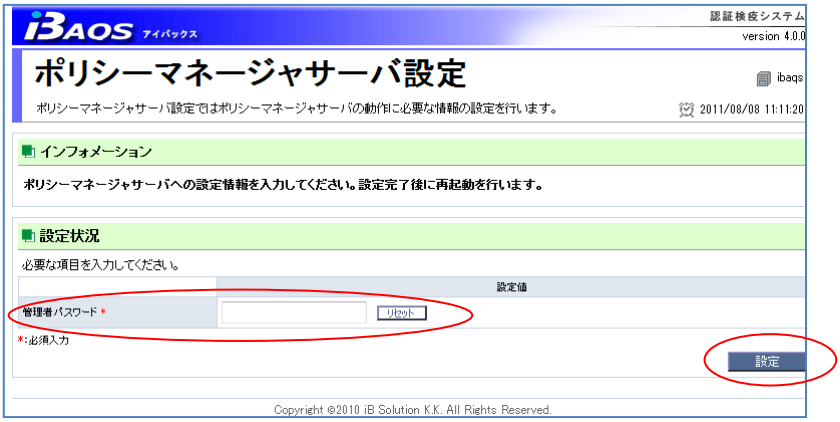
④ **ポリシーマネージャサーバに接続する際のパスワードを設定します**

[⚠ご注意]

ポリシーマネージャコンソールで接続する際に使用しますので忘れないようにしてください。

[メモ]

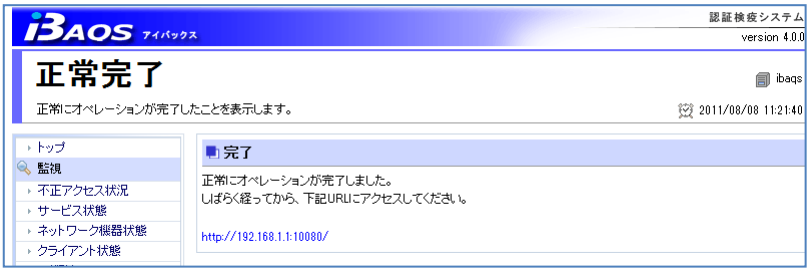
当画面は初めてのログイン時に表示されます。設定が完了すると表示されなくなります。



⑤ **正常完了画面が表示されます。**

[⚠ご注意]

自動的に再起動が行われます。



ライセンスキー登録

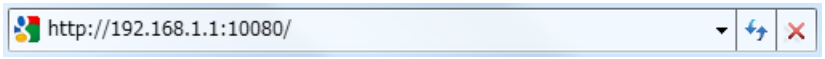
本製品にライセンスキーを登録する手順を以下に示します。

[⚠ご注意]

お手元にライセンス証書をご用意ください。

① **iBAQS と設定用のパソコンを同じスイッチ(ハブ)に接続し、iBAQS の電源を入れます。**

② **ブラウザを使用して http://192.168.1.1:10080/または http://[インストール時に設定した IP アドレス]:10080/を開きます**



③ **管理者 ID でログインします**

[メモ]

初期の管理者 ID は【manager】、管理者パスワードは【friend】です

④ **ライセンス証書に記載されているライセンスキーを登録します**

[ご注意]

「キャンセル」を選択した場合は、ライセンスキーの登録を中止します。

⑤ **トップ画面が表示されます。**

[ご注意]

アプライアンス版またはインターネットに接続できない環境に設置したソフトウェア版でライセンスキーを登録すると、管理システム接続エラーが表示されますが異常ではありません。「OK」をクリックしてトップ画面へ進んでください。

[メモ]

管理システムとはアイビーソリューション株式会社のアップデートサーバを指します。

以上でライセンスキー登録は終了です。

各部の名称と機能

ここでは本製品の各部の名称と機能を説明します。

全体構成

全体構成は次の通りです。

画面は 3 つの部分となる①ヘッダ、②メニュー、③メインから成り立っています。

ヘッダ

①ヘッダには、iBAQS のバージョン、現在表示している画面の名称、ホスト名、現在日時を表示します。

メニュー

②メニューの構成は次の通りです。

メニュー		説明
メイン	サブ	
監視	MAC 収集状況	収集した MAC アドレスの確認、エクスポート、削除を行います。
	不正アクセス状況	未登録でのアクセス状況や過去に削除した不正アクセス状況を表示します。
	サービス状態	各サービスの動作状態を表示します。
	ネットワーク機器状態	ネットワーク機器の動作状況を表示します。
	クライアント状態	クライアントの認証／AVS 確認／接続状態を表示します。
	ログ監視	各種ログの閲覧やエクスポートを行います。
設定	サーバ設定	サーバの基本設定を行います。
	冗長化設定	冗長化情報の設定を行います。
	システム設定	iBAQS のシステム設定を行います。
	ライセンス設定	iBAQS のライセンス設定を行います。
	外部連携設定	外部との連携機能設定を行います。
	管理者設定	管理者の設定を行います。
	証明書設定	認証局やクライアント証明書に関する設定を行います。
	DHCP 設定	DHCP サーバに関する設定を行います。
	クライアント設定	クライアントに関する設定を行います。
	ネットワーク機器設定	ネットワーク機器に関する設定を行います。
	スケジュール設定	定期的に処理するプログラムのスケジュール設定を行います。
	バックアップ設定	データベースのバックアップ情報の設定を行います。
	リストア	システム全体の復元を行います。
	アップデート	アップデート可能かどうかを確認し、アップデートを行います。

メニュー		説明
メイン	サブ	
管理	ハードウェア状態	現在のハードウェア状態を表示します。
	通信確認	ping, traceroute, nslookup のコマンドが利用可能です。
	オンライン マニュアル	本マニュアルを表示します。
	ログアウト	ログアウトを行います。

メイン

③メインには、メニューで選択した画面を表示します。各画面の内容は次章以降を参照してください。

監視

トップ.....29
MAC 収集状況.....33
不正アクセス状況.....34
サービス状態.....36
ネットワーク機器状態.....38
通信制限状況.....39
クライアント状態.....40
ログ監視.....43
認証ログ.....45
AVS 確認ログ.....47
管理ログ.....49

トップ

トップでは各種サマリー情報が表示されます。
各項目に用意されているリンクのアイコンをクリックすることで詳細を確認できます。

- インフォメーション

  インフォメーションにはシステム全体の異常有無を表示します。

- システム状況

<table>
<tr><th>項目名</th><th colspan="3"></th></tr>
<tr><td rowspan="5">ライセンス有効期限</td><td colspan="3">現在登録されているライセンスの有効期限を表示します。
有効期限が切れるとアップデート等が利用できなくなります。</td></tr>
<tr><td>状態</td><td>詳細</td><td>意味</td></tr>
<tr><td>正常</td><td>YYYY/MM/DD</td><td>有効期限まで 31 日以上ある状態</td></tr>
<tr><td>警告</td><td>YYYY/MM/DD
（期限切れまであと x 日）</td><td>有効期限まで 30 日以内の状態</td></tr>
<tr><td rowspan="2">異常</td><td>YYYY/MM/DD
（期限切れ）</td><td>有効期限切れの状態</td></tr>
<tr><td>未取得</td><td>有効期限を取得していない状態</td></tr>
</table>

<table>
<tr><th>項目名</th><th colspan="3"></th></tr>
<tr><td>AVS 用パターンファイル</td><td colspan="3">内蔵するエフセキュア ポリシーマネージャサーバの持つパターンファイルの状態を表示します。
詳細な状態はポリシーマネージャコンソールを使用してご確認ください。
※「AVS」とは「アンチウイルスソフト」の略称です。</td></tr>
<tr><td></td><td>状態</td><td>詳細</td><td>意味</td></tr>
<tr><td></td><td>正常</td><td>YYYY-MM-DD_NN</td><td>2 日以内に更新されている状態</td></tr>
<tr><td></td><td>警告</td><td>YYYY/MM/DD_NN
(N 日経過)</td><td>3 日～6 日更新されていない状態</td></tr>
<tr><td></td><td rowspan="2">異常</td><td>YYYY/MM/DD_NN
(N 日経過)</td><td>7 日以上更新されていない状態</td></tr>
<tr><td></td><td>(形式エラー)</td><td>パターンファイルの状態を確認出来ない状態</td></tr>
<tr><td>冗長化運転
(冗長構成時のみ表示)</td><td colspan="3">冗長構成のステータスを表示します。
警告の場合にはピアサーバの動作を確認してください。
異常の場合にはピアサーバを起動したまま再起動することで切替運転のセカンダリとして復帰可能な場合があります。</td></tr>
<tr><td></td><td>状態</td><td>詳細</td><td>意味</td></tr>
<tr><td></td><td rowspan="2">正常</td><td>通常運転中です</td><td>設定通りの冗長構成で動作している状態</td></tr>
<tr><td></td><td>切替運転中です</td><td>設定とは逆に冗長構成で動作している状態</td></tr>
<tr><td></td><td>警告</td><td>縮退運転中です</td><td>ピアサーバが存在しない（接続できない）状態</td></tr>
<tr><td></td><td>異常</td><td>異常が発生しています</td><td>ピアサーバとの接続に問題がある状態</td></tr>
</table>

<table>
<tr><th>項目名</th><th colspan="3"></th></tr>
<tr><td>ミラーディスク
（冗長構成時のみ表示）</td><td colspan="3">ミラーディスクの状態を表示します。
強制同期中は再起動、シャットダウンを伴う操作は抑制されます。
状態が異常の場合、単独で起動してもプライマリで動作できません。
ピアサーバを準備し、ピアサーバと強制同期を完了させてください。
ピアサーバと強制同期が完了できない場合にはミラーディスクの物理的な破損の可能性があります。
<table>
<tr><th>状態</th><th>詳細</th><th>意味</th></tr>
<tr><td rowspan="2">正常</td><td>通常同期中です</td><td>正常にミラーリングを行っている状態</td></tr>
<tr><td>強制同期中(NN.N%)</td><td>通常同期に加え、差分同期を行っている状態</td></tr>
<tr><td>警告</td><td>-</td><td>縮退運転でミラーリングを行っていない状態</td></tr>
<tr><td>異常</td><td>-</td><td>ミラーディスクが論理的に破損している状態</td></tr>
</table></td></tr>
<tr><td>MAC 収集状況
(MAC 収集モードのみ表示)</td><td colspan="3">MAC 収集の状態を表示します。
<table>
<tr><th>状態</th><th>詳細</th><th>意味</th></tr>
<tr><td>正常</td><td>N 件収集しました</td><td>収集した MAC アドレスの件数を表示</td></tr>
</table></td></tr>
<tr><td>不正アクセス状況</td><td colspan="3">未対処の不正アクセス有無を表示します。
不正アクセスが検出された場合は詳細を確認し、検出した未登録クライアントを登録するかネットワークから切断して不正アクセス状況画面で削除を行ってください。
不正アクセスが検出された場合でも、検出したネットワーク機器を経由する通信は制限されますので、ネットワークは脅威から保護されています。
<table>
<tr><th>状態</th><th>詳細</th><th>意味</th></tr>
<tr><td>正常</td><td>不正アクセスは
ありません</td><td>未登録クライアントの接続がないか全て対処済の状態</td></tr>
<tr><td>異常</td><td>不正アクセスが
存在します</td><td>未登録クライアントの接続を制限した状態</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>項目名</th><th></th></tr>
<tr><td>サービス状態</td><td>iBAQS で利用しているサービス停止の有無を表示します。
異常が発生している場合にはサービス状態画面で停止しているサービスの起動を試みてください。
冗長構成で認証や AVS 確認に必須のサービスが停止している場合にはフェイルオーバーが発生します。
<table>
<tr><th>状態</th><th>詳細</th><th>意味</th></tr>
<tr><td>正常 </td><td>正常動作中です</td><td>全てのサービスが正常に動作している状態</td></tr>
<tr><td>異常 </td><td>一部停止中です</td><td>1 つ以上のサービスが停止している状態</td></tr>
</table></td></tr>
<tr><td>ネットワーク機器状態</td><td>iBAQS に登録されているネットワーク機器が ping に応答有無を表示します。
異常が発生している場合にはサービス状態画面で停止しているサービスの起動を試みてください。
冗長構成で認証や AVS 確認に必須のサービスが停止している場合にはフェイルオーバーが発生します。
<table>
<tr><th>状態</th><th>詳細</th><th>意味</th></tr>
<tr><td>正常 </td><td>正常動作中です</td><td>全てのネットワーク機器が ping に応答する状態</td></tr>
<tr><td>異常 </td><td>異常が発生しています</td><td>1 つ以上のネットワーク機器が ping に応答しない状態</td></tr>
</table></td></tr>
<tr><td>クライアント登録数</td><td>現在登録されているクライアント数を表示します。
警告でクライアントの追加を予定されている場合にはライセンス数の追加をご検討ください。
<table>
<tr><th>状態</th><th>詳細</th><th>意味</th></tr>
<tr><td>正常 </td><td>N 件登録されています</td><td>ライセンス数が足りている状態</td></tr>
<tr><td>警告 </td><td>N 件登録されています</td><td>登録クライアント数がライセンス数の 90%を超えている状態</td></tr>
</table></td></tr>
</table>

MAC 収集状況

MAC 収集状況は MAC 収集モードが有効の場合のみ表示します。MAC 収集状況では MAC 収集モードにより収集した MAC アドレスの一覧を確認、エクスポート、削除できます。エクスポートはクライアント一括変更形式の CSV ファイルとなり、備考に検出した際の機器 IP アドレスとポート番号を記載しています。機器 IP アドレス、ポート番号の付加情報により該当 MAC アドレスの PC 名、セグメント、IP アドレス等の不足情報収集作業の支援をします。

- インフォメーション

  現在検出した MAC アドレス数を表示します。

- 収集結果

  MAC アドレス数が 50 件を超える場合には、ページング処理が行われ 1 ページあたり 50 件まで表示します。エクスポートボタンで収集結果のダウンロード、一括削除ボタンで収集結果の削除を行えます。

項目名	
初期検出日時	MAC アドレスを初めて検出した日時を表示します。
MAC アドレス	検出した MAC アドレスを表示します。
機器 IP アドレス	MAC アドレスを始めて検出したネットワーク機器の IP アドレスを表示します。
ポート	MAC アドレスを始めて検出したネットワーク機器のポート番号を表示します。

不正アクセス状況

不正アクセス状況画面では未登録の MAC アドレスを持つクライアントがネットワークに接続した状況を確認できます。最後に不正アクセスを検出したネットワーク機器の情報が一目で把握できますので、該当ネットワーク機器の場所へ移動して未登録クライアントの特定が容易になります。検索条件による絞り込みや、登録漏れクライアントの MAC アドレスをクライアント追加へ引き渡すこともできます。

- インフォメーション

  現在の不正アクセス概要を表示します。

- 検索条件

項目名		
ソート	表示対象を検出日時でソートします。降順、昇順から選択できます。デフォルトは降順です。	
	設定値	動作
	降順	検出日時の新しいものから順に表示します。
	昇順	検出日時の古いものから順に表示します。

<table>
<tr><th>項目名</th><th colspan="2"></th></tr>
<tr><td>検出日時</td><td colspan="2">表示対象の期間を指定します。デフォルトでは開始日、終了日共に設定なしで全期間が表示対象です。開始日のみ、終了日のみの指定もできます。カレンダーのアイコン をクリックすることでポップアップカレンダーが表示され、視覚的に日時を選択することもできます。</td></tr>
<tr><td></td><td>設定値</td><td>動作</td></tr>
<tr><td></td><td>開始日</td><td>入力した開始日の 0 時 0 分からを対象とします。</td></tr>
<tr><td></td><td>終了日</td><td>入力した終了日の 23 時 59 分までを対象とします。</td></tr>
<tr><td>確認状態</td><td colspan="2">表示対象の確認状態を指定します。デフォルトは未確認です。</td></tr>
<tr><td></td><td>設定値</td><td>動作</td></tr>
<tr><td></td><td>未確認</td><td>対処の完了していない不正クライアントを表示します。</td></tr>
<tr><td></td><td>登録済</td><td>不正アクセス状況画面の登録ボタン、クライアント設定の新規追加、CSV 一括処理のいずれかの方法で登録を行ったクライアントを表示します。</td></tr>
<tr><td></td><td>削除済</td><td>ネットワークから切断し、削除処理を行った未登録クライアントを表示します。</td></tr>
</table>

- 検索結果

項目名	
エクスポートボタン	確認状態が未確認の場合のみ表示します。エクスポートボタンをクリックすると CSV 一括登録の形式で MAC アドレスの一覧を出力することができます。
検出日時	最後に検出された日時を表示します。
初期検出日時	最初に検出された日時を表示します。
MAC アドレス	検出した未登録クライアントの MAC アドレスを表示します。
確認状態	検索条件で指定した確認状態を表示します。
登録	確認状態が未確認の場合のみクライアント追加へのリンクを表示します。登録をクリックすると MAC アドレスの入力が不要になります。
機器名	最後に不正アクセスを検出したネットワーク機器の機器名を表示します。
設置場所	最後に不正アクセスを検出したネットワーク機器の設置場所を表示します。
機器 IP アドレス	最後に不正アクセスを検出したネットワーク機器の IP アドレスを表示します。
ポート	最後に不正アクセスを検出したネットワーク機器のポート番号を表示します。
削除	確認状態が未確認の場合のみリンクを表示します。削除をクリックすると該当クライアントの確認状態を「削除済」に変更します。

サービス状態

サービス状態では iBAQS の動作に必要なサービスの稼働状況を確認できます。何らかの理由でサービスが停止している場合には起動ボタンにより起動を試みることができます。
※冗長構成時に冗長対象のサービスが停止するとフェイルオーバーが発生します。

- インフォメーション

  サービス全体の動作概要を表示します。

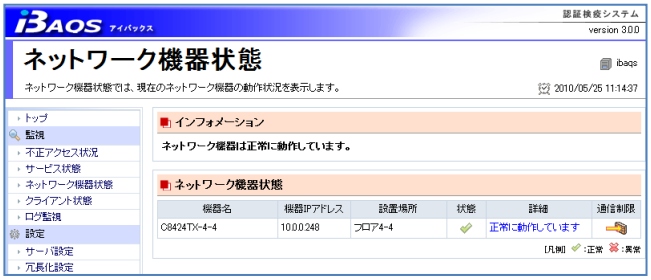
- サービス状態

  サービスの稼働状況を状態に正常 、異常 で表示します。異常 のサービスは起動に表示される起動ボタンで起動できます。冗長構成時には冗長監視サービスがフェイルオーバー対象のサービスを約 10 秒に 1 回監視しており、異常が発生すると約 5 秒に 1 回の監視に切り替わります。連続で 3 回異常を確認した場合にはシャットダウンを行い、ピアサーバに業務を引き継ぎます。縮退運転時にはスタンドアロンと同じ動作となり、シャットダウンは行われません。

項目	説明	フェイルオーバー
DHCP	クライアントにIPアドレスやDNSの情報を払い出します。	対象
NTP	iBAQSの時刻を上位のntpサーバに同期します。	-
LDAP		対象
データベース	設定情報やログが格納されています。	対象
RADIUS	ネットワーク機器からの認証要求に応答します。	対象
エフセキュア ポリシーマネージャ サーバ	AVSの集中管理サーバです。パターンファイルやポリシーデータ（設定情報）の配信を行います。	対象
エフセキュア自動更新 エージェント	インターネットからパターンファイルをダウンロードし、ポリシーマネージャサーバに対して配信を行います。	対象
同期サービス	ミラーディスクを提供します。冗長構成時にはピアサーバと接続してミラーディスクの内容を常時同期します。	-
冗長監視サービス	フェイルオーバー対象のリソース制御を行います。冗長構成時にはピアサーバの死活監視やリソース監視を行います。	-
不正アクセス検出 サービス	認証ログの失敗の中から未登録クライアントの抽出を行い、不正アクセス状況の更新、アラートメールの送信を行います。	対象
アンチウイルスソフト 確認開始サービス	認証ログの成功の中から AVS 確認対象クライアントの抽出を行い、ACL 制御サービスに隔離要求を行います。	対象
アンチウイルスソフト 確認完了サービス	ポリシーマネージャサーバのログから AVS の動作状況を取得し、ACL 制御サービスに隔離解除要求を行います。また、AVS 確認時間の更新も行います。	対象
ACL 制御サービス	認証スイッチと telnet で接続し、フィルタを定義、削除することで隔離、隔離解除を行います。	対象
UPS 制御サービス （UPS 連携時）	UPS と通信を行い、UPS が商用電源の異常を検出するとシャットダウンを行います。	-
SNMP ｴｰｼﾞｪﾝﾄｻｰﾋﾞｽ （SNMP 連携時）	SNMP エージェントとして動作し、各種情報を SNMP マネージャに提供します。	-

ネットワーク機器状態

ネットワーク機器状態では登録されているネットワーク機器に対して定期的に行っている ping による通信確認の結果を確認することができます。また、各ネットワーク機器に適用されている通信制限の状況を確認する画面へのリンクを提供します。



- インフォメーション

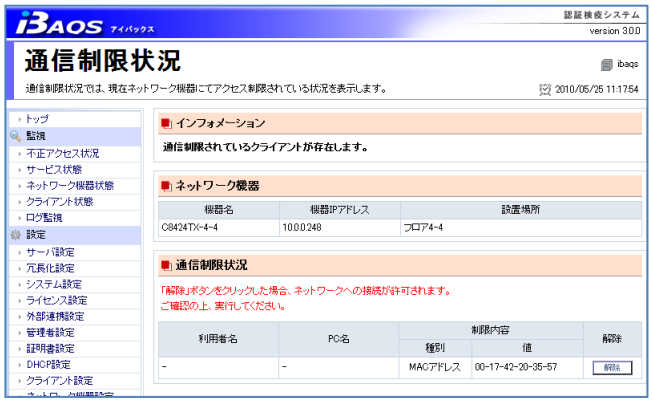
  ネットワーク機器全体の稼働状態概要を表示します。

- ネットワーク機器状態

項目	説明		
機器名	ネットワーク機器登録時に選択した機器名（機種名）が表示されます。		
機器 IP アドレス	ネットワーク機器の IP アドレスを表示します。		
設置場所	ネットワーク機器登録時に入力した設置場所が表示されます。		
状態、詳細	ネットワーク機器の異常有無を表示します。		
	状態	詳細	意味
	正常	正常に動作しています。	直前に行われたネットワーク機器監視処理の ping に応答する状態
	異常	異常が発生しています。	直前に行われたネットワーク機器監視処理の ping に応答しない状態
通信制限	アイコンをクリックすることで、該当機器に現在適用されている通信制限の状況を表示します。ネットワーク機器に異常が発生している場合にはアイコンは表示されません。		

通信制限状況

通信制限状況ではネットワーク機器に定義されているアクセス制限の状況を表示します。



- インフォメーション

  インフォメーションには通信制限されているクライアントの有無を表示します。

- ネットワーク機器状態

表示対象のネットワーク機器名、機器 IP アドレス、設置場所を表示します。

- 通信制限状況

項目	説明
利用者名	通信が制限されているクライアントの利用者名を表示します。未登録の MAC アドレスの場合には"-"（ハイフン）を表示します。
PC 名	通信が制限されているクライアントの利用者名を表示します。未登録の MAC アドレスの場合には"-"（ハイフン）を表示します

項目	説明	
制限内容	種別	CentreCOM 8600 シリーズ、CentreCOM 8700 シリーズは IP アドレス、それ以外の機種では MAC アドレスとなります。
	値	制限対象の MAC アドレスまたは IP アドレスを表示します。
解除	解除ボタンをクリックするとネットワーク機器に定義されたフィルタを削除します。AVS 確認をしないクライアントをするとして登録してしまい、制限されたような場合にはクライアント設定の修正後に解除ボタンを利用して通信可能にしてください。	

クライアント状態

クライアント状態では AVS 確認を行うクライアントの接続状態を確認できます。

- インフォメーション

  インフォメーションには AVS 確認対象のクライアント数が表示されます。

- 検索条件

<table>
<tr><th>項目</th><th colspan="2">説明</th></tr>
<tr><td>検索文字列</td><td colspan="2">利用者名または PC 名から指定した文字列を含むクライアントを検索します。
デフォルトは空白で絞り込みを行いません。
半角全角問わず最大 50 文字まで指定可能で、部分一致検索です。
長い文字列を入力した場合には全体を表示できない場合がありますので、カーソルキー等を利用してスクロールしてください。</td></tr>
<tr><td rowspan="4">ステータス</td><td colspan="2">クライアントの接続状態によって絞り込みを行います。</td></tr>
<tr><td>設定値</td><td>動作</td></tr>
<tr><td>未認証で AVS 未確認</td><td>接続されていないクライアントを表示します。
対象の条件は一度も認証および AVS 確認が行われていないクライアント、最終の認証または AVS 確認からシステム設定の AVS 確認不要時間で設定した時間を経過したクライアントです。</td></tr>
<tr><td>認証済で AVS 未確認</td><td>通信制限を受けているクライアントを表示します。
対象の条件は認証が完了し、AVS 確認が完了していないクライアントです。</td></tr>
<tr><td></td><td>認証済で AVS 確認済</td><td>接続されているクライアントを表示します。
対象の条件は認証、AVS 確認共に完了しているクライアントです。</td></tr>
</table>

- 検索結果

項目	説明
利用者名	利用者名を表示します。
PC 名	PC 名を表示します。

項目	説明	
ステータス	クライアントの現在の接続状態を表示します。	
		説明
	未認証で AVS 未確認	接続されていないクライアントです。一度も認証および AVS 確認が行われていないクライアント、最終の認証または AVS 確認からシステム設定の AVS 確認不要時間で設定した時間を経過したクライアントです。
	認証済で AVS 未確認	通信制限を受けているクライアントです。認証が完了し、AVS 確認が完了していないクライアントです。
	認証済で AVS 確認済	接続されているクライアントです。認証、AVS 確認共に完了しているクライアントです。
認証	認証状態を表示します。	
	アイコン	意味
	—	一度も認証を受けたことがないか、最終の認証日時または AVS 確認日時からシステム設定の AVS 確認不要時間の設定値を経過している状態です。ネットワーク利用には認証、AVS 確認が必要になります。
		認証を受け、最終の認証日時または AVS 確認日時からシステム設定の AVS 確認不要時間の設定値を経過していない状態です。
AVS	AVS 確認状態を表示します。	
	アイコン	意味
	—	一度も AVS 確認を受けたことがないか、AVS 確認日時からシステム設定の AVS 確認不要時間の設定値を経過している状態です。 ネットワーク利用には AVS 確認が必要になります。
		AVS 確認を受け、最終の認証日時または AVS 確認日時からシステム設定の AVS 確認不要時間の設定値を経過していない状態です。
認証日時	最後に認証を受けた日時を表示します。認証に失敗した場合には"-"（ハイフン）に変化します。	
AVS 確認日時	最後に AVS 確認を受けた日時を表示します。AVS 確認不要時間の設定値を経過して新たに認証を受け付けた場合には"-"（ハイフン）に変化します。	

ログ監視

ログ監視では各種ログへのリンク、各種ログのエクスポート機能を提供します。

- インフォメーション

  インフォメーションには説明が表示されます。

- 各種ログ 閲覧

項目	説明
認証ログ 	認証ログ画面へ移動します。 認証ログ画面ではクライアントの認証履歴を一覧で表示します。
AVS 確認ログ 	AVS 確認ログ画面へ移動します。 AVS 確認ログ画面ではクライアントの AVS 確認履歴を一覧で表示します。
管理ログ 	管理ログ画面へ移動します。 管理ログ画面では管理画面でのオペレーション履歴を一覧で表示します。

- 各種ログ エクスポート

  各種ログを CSV ファイルとしてエクスポートすることができます。

項目	説明	
ログファイル	エクスポート対象のログを選択します。	
	設定値	動作
	認証ログ	認証ログをエクスポートします。
	AVS 確認ログ	AVS 確認ログをエクスポートします。
	管理ログ	管理ログをエクスポートします。
日付	エクスポート対象の期間を入力します。デフォルトでは開始日、終了日共に設定なしで全期間が表示対象です。開始日のみ、終了日のみの指定もできます。カレンダーのアイコン をクリックすることでポップアップカレンダーが表示され、視覚的に日時を選択することもできます。	
	開始日	入力した開始日の 0 時 0 分からを対象とします。
	終了日	入力した終了日の 23 時 59 分までを対象とします。

認証ログ

認証ログではクライアントが認証を受けた履歴を一覧で確認することができます。また、多彩な検索機能により目的の履歴をピンポイントで表示することもできます。

- 検索条件

項目	説明	
検索モード	検索する方法を指定します。	
	設定値	動作
	最新 100 件を降順で表示する	絞り込みを行わず最新 100 件を新しい順に表示します。
	下記条件で検索表示する	ソート、認証日付、検索文字列、認証結果による絞り込みを行い、該当するログを全件表示します。1 ページの最大表示件数は 100 件です。
ソート	表示対象を検出日時でソートします。降順、昇順から選択できます。デフォルトは降順です。	
	設定値	動作
	降順	検出日時の新しいものから順に表示します。
	昇順	検出日時の古いものから順に表示します。

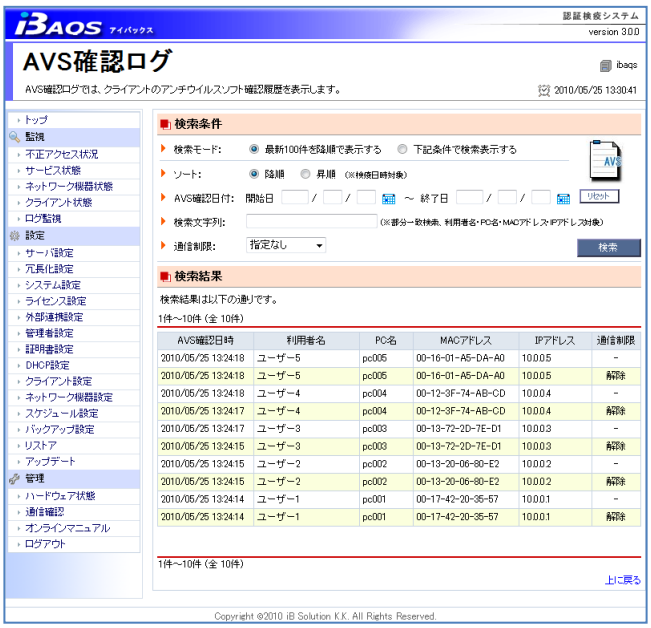
<table>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>検出日時</td><td>表示対象の期間を指定します。デフォルトでは開始日、終了日共に設定なしで全期間が表示対象です。開始日のみ、終了日のみの指定もできます。カレンダーのアイコン をクリックすることでポップアップカレンダーが表示され、視覚的に日時を選択することもできます。
<table>
<tr><th>設定値</th><th>動作</th></tr>
<tr><td>開始日</td><td>入力した開始日の 0 時 0 分からを対象とします。</td></tr>
<tr><td>終了日</td><td>入力した終了日の 23 時 59 分までを対象とします。</td></tr>
</table></td></tr>
<tr><td>検索文字列</td><td>ユーザーID、MAC アドレス、PC 名から指定した文字列を含むログを検索します。
デフォルトは空白で絞り込みを行いません。
半角全角問わず最大 50 文字まで指定可能で、部分一致検索です。
長い文字列を入力した場合には全体を表示できない場合がありますので、カーソルキー等を利用してスクロールしてください。</td></tr>
<tr><td>認証結果</td><td>表示対象の確認状態を指定します。デフォルトは指定なしです。
<table>
<tr><th>設定値</th><th>動作</th></tr>
<tr><td>指定なし</td><td>認証結果が成功、失敗ともに表示します。</td></tr>
<tr><td>成功</td><td>認証結果が成功のみを表示します。</td></tr>
<tr><td>失敗</td><td>任所結果が失敗のみを表示します。</td></tr>
</table></td></tr>
</table>

- 検索結果

項目	説明
認証日時	認証を受けた日時を表示します。
結果	認証の結果を成功、失敗で表示します。
ユーザーID	認証に利用されたユーザーID を表示します。
MAC アドレス	クライアントの MAC アドレスを表示します。 RADIUS の要求に含まれている Calling-Station-Id を記録しています。
PC 名	認証を受けたクライアントが登録済であれば PC 名が表示されます。未登録であれば"-"（ハイフン）を表示します。
機器 IP アドレス	認証を受けたネットワーク機器の IP アドレスを表示します。
ポート	認証を受けたネットワーク機器のポート番号を表示します。

AVS 確認ログ

AVS 確認ログでは AVS が動作していることを確認した履歴を表示します。
AVS 確認は IP アドレスベースで行われるため、キーとなる情報は IP アドレスになります。



- 検索条件

項目	説明	
検索モード	検索する方法を指定します。	
	設定値	動作
	最新 100 件を降順で表示する	絞り込みを行わず最新 100 件を新しい順に表示します。
	下記条件で検索表示する	ソート、AVS 確認日付、検索文字列、通信制限による絞り込みを行い、該当するログを全件表示します。1 ページの最大表示件数は 100 件です。
ソート	表示対象を検出日時でソートします。降順、昇順から選択できます。デフォルトは降順です。	
	設定値	動作
	降順	検出日時の新しいものから順に表示します。
	昇順	検出日時の古いものから順に表示します。

<table>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>検出日時</td><td>表示対象の期間を指定します。デフォルトでは開始日、終了日共に設定なしで全期間が表示対象です。開始日のみ、終了日のみの指定もできます。カレンダーのアイコン をクリックすることでポップアップカレンダーが表示され、視覚的に日時を選択することもできます。
<table>
<tr><th>設定値</th><th>動作</th></tr>
<tr><td>開始日</td><td>入力した開始日の 0 時 0 分からを対象とします。</td></tr>
<tr><td>終了日</td><td>入力した終了日の 23 時 59 分までを対象とします。</td></tr>
</table></td></tr>
<tr><td>検索文字列</td><td>利用者名、PC 名、MAC アドレス、IP アドレスから指定した文字列を含むログを検索します。デフォルトは空白で絞り込みを行いません。
半角全角問わず最大 50 文字まで指定可能で、部分一致検索です。
長い文字列を入力した場合には全体を表示できない場合がありますので、カーソルキー等を利用してスクロールしてください。</td></tr>
<tr><td>通信制限</td><td>表示対象の通信制限に関する処理内容を指定します。デフォルトは指定なしです。
<table>
<tr><th>設定値</th><th>動作</th></tr>
<tr><td>指定なし</td><td>"-"（ハイフン）、解除ともに表示します。</td></tr>
<tr><td>-</td><td>通常の AVS 確認のみを表示します。</td></tr>
<tr><td>解除</td><td>通信制限解除対象の AVS 確認のみを表示します。</td></tr>
</table></td></tr>
</table>

- 検索結果

項目	説明
AVS 確認日時	AVS 確認を受けた日時を表示します。
利用者名	AVS 確認を受けたクライアントの利用者名を表示します。 クライアント設定で入力した IP アドレスに対応する利用者名を表示します。
PC 名	AVS 確認を受けたクライアントの PC 名を表示します。 クライアント設定で入力した IP アドレスに対応する PC 名を表示します。
MAC アドレス	クライアントの MAC アドレスを表示します。 クライアント設定で入力した IP アドレスに対応する MAC アドレスを表示します。
IP アドレス	クライアントの IP アドレスを表示します。 AVS 確認のキーとなる情報です。本情報は FSPMS から取得します。

項目	説明	
通信制限	AVS 確認後に通信制限に対して行われた処理内容を表示します。	
	内容	詳細
	–	最終 AVS 確認時間の延長のみで通信制限解除は行っていないことを表します。
	解除	AVS 確認により通信制限が解除されたことを表します。

管理ログ

管理ログでは管理画面で行われたオペレーションの履歴を確認することができます。

- 検索条件

<table>
<tr><th>項目</th><th colspan="2">説明</th></tr>
<tr><td rowspan="4">検索モード</td><td colspan="2">検索する方法を指定します。</td></tr>
<tr><td>設定値</td><td>動作</td></tr>
<tr><td>最新 100 件を
降順で表示する</td><td>絞り込みを行わず最新 100 件を新しい順に表示します。</td></tr>
<tr><td>下記条件で
検索表示する</td><td>ソート、AVS 確認日付、検索文字列、通信制限による絞り込みを行い、該当するログを全件表示します。1 ページの最大表示件数は 100 件です。</td></tr>
<tr><td rowspan="4">ソート</td><td colspan="2">表示対象を検出日時でソートします。降順、昇順から選択できます。デフォルトは降順です。</td></tr>
<tr><td>設定値</td><td>動作</td></tr>
<tr><td>降順</td><td>検出日時の新しいものから順に表示します。</td></tr>
<tr><td>昇順</td><td>検出日時の古いものから順に表示します。</td></tr>
<tr><td rowspan="4">日時</td><td colspan="2">表示対象の期間を指定します。デフォルトでは開始日、終了日共に設定なしで全期間が表示対象です。開始日のみ、終了日のみの指定もできます。カレンダーのアイコン をクリックすることでポップアップカレンダーが表示され、視覚的に日時を選択することもできます。</td></tr>
<tr><td>設定値</td><td>動作</td></tr>
<tr><td>開始日</td><td>入力した開始日の 0 時 0 分からを対象とします。</td></tr>
<tr><td>終了日</td><td>入力した終了日の 23 時 59 分までを対象とします。</td></tr>
</table>

- 検索結果

項目	説明
日時	操作を行った日時を表示します。
ログ内容	操作の内容を表示します。

設定

サーバ設定 53
冗長化設定 56
システム設定 58
ライセンス設定 62
外部連携設定 64
UPS 連携設定 65
SNMP マネージャ連携設定 66
管理者設定 68
証明書設定 70
認証局編集 72
クライアント証明書発行 74
クライアント証明書ダウンロード . . . 76
DHCP 設定 78
セグメント追加 80
セグメント編集 82
セグメント削除 84

設定

クライアント設定.....85
クライアント追加.....87
クライアント一括変更.....90
クライアント一括削除.....95
クライアント編集.....96
クライアント削除.....99
ネットワーク機器設定.....101
ネットワーク機器追加.....103
ネットワーク機器編集.....105
ネットワーク機器削除.....107
スケジュール設定.....108
バックアップ設定.....111
リストア.....114
アップデート.....116

サーバ設定

サーバ設定では IP アドレスやホスト名等、固有の設定内容を変更できます。基本、その他、再起動、シャットダウンのタブを用意しており、再起動、シャットダウンタブでは iBAQS の再起動、シャットダウンを行うためのボタンを設けています。

- インフォメーション

  操作の概要を表示します。

- 設定状況

項目	説明	
使用 LAN インターフェース	RADIUS が待ち受けを行うインターフェースを指定します。再起動等で表示されるリンクも指定したインターフェースの IP アドレスで表示されます。	
	設定値	意味
	eth[n]	iBAQS を後ろから見て左から n+1 番目の RJ-45 コネクタを RADIUS 待ち受けインターフェースとして使用します。
eth[n]	iBAQS を後ろから見て左から n+1 番目の RJ-45 コネクタに対するネットワーク情報を設定します。	
	設定値	動作
使用	する	インターフェースを使用します。IP アドレス、サブネットマスクの入力が必要になります。
	しない	インターフェースを使用しません。IP アドレス、サブネットマスクの入力は不要です。少なくとも 1 つのインターフェースは使用するに設定する必要があります。
IP アドレス	IPv4 アドレス	ネットワークアドレスやブロードキャストアドレス、ネットワーク機器やクライアント等と重複する IP アドレスは設定できません。デフォルトは 192.168.1.1 です。
サブネットマスク	IPv4 サブネットマスク	ネットワーク空間の大きさを決めるサブネットマスクを設定します。不正な値が入力された場合にはエラーとなります。デフォルトは 255.255.255.0 です。
デフォルトゲートウェイ	他のセグメントと通信する際に利用するルータのアドレスを設定します。 デフォルトは 192.168.1.254 です。	
ログ内容	操作の内容を表示します。	
ホスト名	ホスト名を設定します。冗長構成時にはピアサーバと重複しないように設定してください。デフォルトは ibaqs です。	
セッションタイマー時間	管理画面の無操作によるタイムアウト時間を設定します。デフォルトは 30 分です。	
DNS	iBAQS が利用する DNS サーバを設定します。Primary は必須入力です。Secondary を入力せずに Tertiary を入力した場合、設定後に設定値は Secondary に反映されます。デフォルトは 192.168.1.254 です。	

項目	説明	
タイムサーバ	iBAQS が時刻同期に使用する NTP サーバを設定します。1 は必須入力です。2 を入力せずに 3 を入力した場合、設定後に設定値は 2 に反映されます。デフォルトは 192.168.1.254 です。	
プロキシサーバ	iBAQS がアップデートサーバと通信する際に使用するプロキシサーバを設定します。デフォルトはプロキシサーバを使用しません。	
	設定値	動作
使用	する	プロキシサーバを使用します。ホスト、ポートの入力は必須です。
	しない	プロキシサーバを使用しません。ホスト、ポートの入力は不要です。
ホスト	IPv4 アドレス または FQDN	使用がするの場合に設定値のプロキシサーバを利用します。デフォルトは空白です。
ポート	1-65535	使用がするの場合に設定値のポート番号を利用します。デフォルトは空白です。

冗長化設定

冗長化設定では冗長構成に必要な情報の設定を行います。iBAQS ではアクティブ-スタンバイ型の冗長構成をサポートします。アクティブ状態で動作している iBAQS をプライマリ、スタンバイ状態で動作している iBAQS をセカンダリと表現します。共有が必要な設定、ログに関してはネットワーク経由で常時ミラーリングされ、リソースに異常が発生した場合にはプライマリ機がシャットダウンすることによりセカンダリ機にフェイルオーバーを行い、認証処理を続けます。リソースチェックは約 10 秒に 1 回行われ、異常発生時には約 5 秒に 1 回に行います。異常発生を 3 回連続で検出するとフェイルオーバーを行います。iBAQS を 1 台で使用する際には設定不要です。冗長化を構成する場合には 2 台のサーバの IP アドレス等の設定を終えてからプライマリとなるサーバ側から冗長化の設定を有効にしてください。セカンダリとなるサーバの設定はプライマリ側から自動的に行われますのでセカンダリとなるサーバでの設定は不要です。冗長化を設定する際にサーバの再起動やシャットダウン操作は不要です。冗長構成で運用する場合にはネットワーク機器の RADIUS サーバ、DHCP リレーエージェントの参照先として仮想 IP アドレスを設定します。
※DHCP リレーエージェントによっては双方のサーバの実 IP アドレスを指定しなければならない場合があります。

- インフォメーション

  操作の概要を表示します。

- 設定状況

<table>
<tr><th>項目</th><th colspan="2">説明</th></tr>
<tr><td rowspan="4">冗長化</td><td colspan="2">冗長化を行うか設定を行います。デフォルト値はしないです。</td></tr>
<tr><td>設定値</td><td>動作</td></tr>
<tr><td>する</td><td>冗長化を行います。通信インターフェース、ピアサーバ IP アドレス、仮想 IP アドレスは必須入力です。</td></tr>
<tr><td>しない</td><td>冗長化を行いません。</td></tr>
<tr><td rowspan="3">通信インターフェース</td><td colspan="2">ミラーディスクの同期やピアサーバの死活確認に利用するインターフェースを選択します。サーバ設定の使用 LAN インターフェースと異なるインターフェースを指定することをおすすめします。使用 LAN インターフェースと通信インターフェースが異なる場合には接続確認 IP アドレスの入力が必須となります。</td></tr>
<tr><td>設定値</td><td>動作</td></tr>
<tr><td>eth[n]</td><td>eth[n]を通信インターフェースとして利用します。通信インターフェースには使用 LAN インターフェースと異なるインターフェースの設定を推奨します。</td></tr>
<tr><td>ピアサーバ IP アドレス</td><td colspan="2">冗長化を構成するピアサーバの IP アドレスを指定します。</td></tr>
<tr><td>仮想 IP アドレス</td><td colspan="2">障害発生時にネットワーク機器の RADIUS サーバ指定やアンチウイルスソフトの管理サーバ指定を変更せずともシームレスに認証/AVS 確認処理が継続できるように共通の IP アドレスを設定します。</td></tr>
<tr><td>接続確認 IP アドレス</td><td colspan="2">使用 LAN インターフェースと通信インターフェースが異なる場合、使用 LAN インターフェース側の障害を確実に検出するために接続確認 IP アドレスに対して ping を行い、正常に接続可能か確認を行います。接続確認 IP アドレスからの応答が無くなるとその他のリソース異常と同様にフェイルオーバーが発生します。ルータや L3 スイッチ等の IP アドレスを指定してください。</td></tr>
</table>

システム設定

システム設定では iBAQS の動作に関連する設定を行います。

- インフォメーション

  操作の概要を表示します。

- 設定状況

項目	説明	
MAC 収集モード	MAC 収集モードを利用するとネットワーク機器を MAC ベース認証設定で配置するだけでネットワーク機器配下に接続されているクライアントの MAC アドレスを収集することができます。この際、クライアント側で設定変更を行う必要はありません。具体的には MAC ベース認証の認証要求に対して全て認証成功を応答し、認証要求に使用された MAC アドレスを収集します。実運用中に MAC 収集モードを有効にすると認証/AVS 確認処理が正しく動作しなくなるのでご注意ください。	
	設定値	動作
	有効	MAC 収集モードを利用します。
	無効	MAC 収集モードを利用しません。

項目	説明	
AVS 確認不要時間	通常、認証後に通信制限が適用され AVS 確認後に通信制限解除という動作になりますが、最終 AVS 確認日時から AVS 確認不要時間を経過していない場合には再び認証が行われた際に通信制限が適用されずにネットワークを利用可能になります。30 分から 1440 分まで指定可能で、デフォルトは 180 分です。	
AVS 確認未完了判定時間	AVS 確認対象クライアントが認証後、AVS 確認未完了判定時間を経過した場合、クライアント通信状態監視処理によりログへの出力、アラートメールの送信が行われます。1 分から 120 分まで指定可能で、デフォルトは 2 分です。クライアント通信状態監視処理が実行されたタイミングで認証済で AVS 未確認のクライアントで指定時間を経過しているクライアントを検出します。	
ログ保持期間	サーバ内にログを蓄積する日数を設定します。0 日から 365 日まで指定可能で、デフォルトは 90 日です。設定日数を越えるログが削除対象となるため、0 日を指定してもログ削除処理実行当日分は削除されません。	
syslog サーバ	RADIUS と DHCP のログを外部の syslog サーバに出力することができます。syslog サーバへの出力を利用するにはホスト、ポート、ファシリティを入力し、使用するに設定します。	
	設定値	動作
使用	する	syslog サーバへのログ出力を行います。
	しない	syslog サーバへのログ出力を行いません。
ホスト	IPv4 アドレス または FQDN	syslog サーバの IP アドレスを設定します。FQDN で指定する場合には通信確認の nslookup から名前解決できることを確認してください。デフォルトは空白です。
ポート	1-65535	syslog サーバの待ち受けポートを指定します。デフォルトは 514 です。
ファシリティ	local0～local6	syslog サーバへ出力する際のファシリティを設定します。デフォルトは local0 です。

項目	説明	
パスワードロック	クライアントがユーザーID による認証を行う場合でかつパスワードの有効期限を設定した場合に指定した日数を経過したクライアントのパスワードをロックします。パスワードがロックされると該当クライアントは認証に失敗しますのでご注意ください。判定はクライアント状態監視処理にて行われます。	
	設定値	動作
パスワードロック	する	パスワードロック機能を利用します。
	しない	パスワードロック機能を使用しません。
日数	0-9999	パスワードロック実行までの猶予期間を設定します。

項目	説明
アラートメール	管理者設定で設定したメールアドレスに対して各状況に応じたアラートメールを送信することができます。
不正アクセスメール	チェックすると未登録クライアントのネットワーク接続を検出した際にアラートメールを送信します。指定した間隔の間に同一クライアントからの不正アクセスが発生した場合には再送を行いません。再送間隔の設定は 0 分から 99 分まで設定できます。デフォルトは 5 分です。0 を指定した場合には検出の都度アラートメールを送信します。
AVS 確認異常動作検出時	チェックするとクライアント通信状態監視処理実行時に AVS 確認未完了時間を経過しているクライアントがあればアラートメールで通知します。
アップデート有の場合	チェックするとアップデート確認処理実行時に新規アップデートを検出するとアラートメールを送信します。
認証有効期限切れ	チェックするとクライアント状態監視処理実行時に指定された日数で認証有効期限の切れるクライアントを検出するとアラートメールを送信します。送信は該当した場合に 1 回のみ行われます。日数は 0 日から 99 日まで設定できます。デフォルトは 7 日です。
パスワード期限切れ（管理者）	チェックするとクライアント状態監視処理実行時に指定された日数でパスワード有効期限の切れるクライアントを検出すると管理者宛にアラートメールを送信します。送信は該当した場合に 1 回のみ行われます。日数は 0 日から 99 日まで設定できます。デフォルトは 3 日です。
パスワード期限切れ（利用者）	チェックするとクライアント状態監視処理実行時に指定された日数でパスワード有効期限の切れるクライアントを検出すると利用者宛にアラートメールを送信します。送信は該当した場合に 1 回のみ行われます。日数は 0 日から 99 日まで設定できます。デフォルトは 7 日です。クライアント設定でメールアドレスが入力されていない場合には送信されません。
認証局/証明書期限切れ	チェックするとクライアント状態監視処理実行時に指定された日数で認証局/証明書の有効期限切れを検出するとアラートメールを送信します。送信は該当した場合に 1 回のみ行われます。日数は 0 日から 99 日まで設定できます。デフォルトは 7 日です。
システム異常時	チェックするとシステムの異常を検出するとアラートメールを送信します。

ライセンス設定

ライセンス設定では登録されているライセンスキー、ライセンス数、ライセンス有効期限を確認、更新することができます。

- インフォメーション

  ライセンスキーの状態を表示します。

- ライセンス有効期限 確認

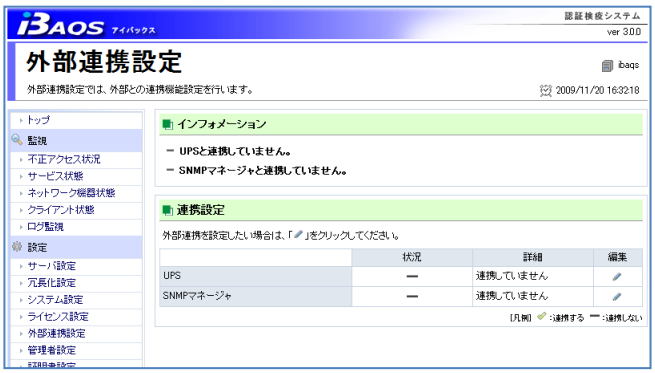
  ライセンス数の変更を伴わずにライセンス有効期限の延長手続きを行われた場合にはライセンスキーは変更となりません。事前に有効期限を反映したい場合には確認ボタンをクリックしてください。アップデートサーバへ http による通信を行いますので、iBAQS が外部と通信できる環境に設置してください。プロキシサーバ経由の確認もできます。インターネットに接続できない環境でご利用になっている場合には別途オフライン用更新ファイルを提供しております。ご希望の方は iBAQS 製品サイトをご覧ください。
  ※オフラインでのご利用はパターンファイルが更新できないため推奨いたしません。

- 設定状況

項目	説明
ライセンスキー	ライセンス証書に記載されているライセンスキーを設定します。アップグレードライセンスを購入された場合にはライセンスキーが変更となりますので、本項目で変更してください。
ライセンス数	登録可能な最大クライアント数を表示します。ライセンス数を増やすにはアップグレードライセンスをご購入いただき、新しいライセンスキーを入手いただきますようよろしくお願いいたします。
ライセンス有効期限	ライセンスキーの有効期限を表示します。ライセンス有効期限が切れますとアップデートやサポートを受けることが出来ません。有効期限の延長に関しては販売店までお問い合わせください。

外部連携設定

外部連携設定では UPS 制御、SNMP マネージャの動作に関して設定を行います。



- インフォメーション

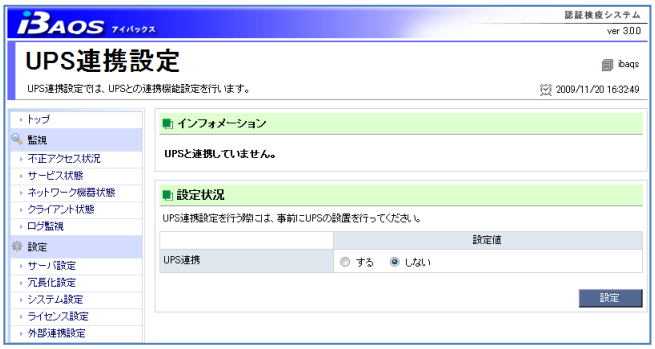
  現在の連携状態を表示します。

- 連携設定

項目	説明		
UPS	UPS 制御の状態確認、設定変更ができます。設定変更は編集のアイコン　をクリックして別画面で行います。		
	状況	詳細	意味
	連携する	連携しています。	UPS 制御を行う設定が有効です。
	連携しない	連携していません。	UPS 制御を行う設定が無効です。
SNMP マネージャ	SNMP マネージャに情報を提供する SNMP エージェントの状態確認、設定変更を行います。設定変更は編集のアイコン　をクリックして別画面で行います。		
	状況	詳細	意味
	連携する	連携しています。	SNMP エージェントは有効です。
	連携しない	連携していません。	SNMP エージェントは無効です。

UPS 連携設定

UPS 連携設定では UPS 制御の設定を変更できます。制御可能なのは APC 社の UPS で Back-UPS、Smart-UPS、CS シリーズ、ES シリーズです。バッテリー運転を 60 秒続けるとシャットダウン処理を開始します。商用電源回復後の自動通電が必要な場合、ES シリーズ以外をご使用ください。iBAQS との接続は USB のみをサポートします。UPS が接続されていない状態で UPS 連携を有効にすることは出来ません。



- インフォメーション

  UPS 連携の状態を表示します。

- 設定状況

項目	説明	
UPS 連携	UPS 連携の有効、無効を設定できます。バッテリー運転を検出してからシャットダウンを開始するまでの時間は 60 秒固定です。USB で接続された APC 社製の UPS が接続されていないときにはするに設定することが出来ません。	
	設定値	動作
	する	UPS 制御ソフトウェアを有効にし、UPS と連携します。
	しない	UPS 制御ソフトウェアを無効にし、UPS と連携しません。

SNMP マネージャ連携設定

SNMP マネージャ連携設定では SNMP エージェントの設定を行います。SNMP マネージャから iBAQS の情報を取得するには SNMP マネージャ連携を有効にしてください。

- インフォメーション

  SNMP マネージャ連携の状態を表示します。

- 設定状況

項目	説明	
SNMP マネージャ連携	SNMP エージェントの有効、無効を設定します。デフォルトはしないです。	
	設定値	動作
	する	SNMP エージェントを有効にし、SNMP マネージャと連携します。
	しない	SNMP エージェントを無効にし、SNMP マネージャと連携しません。

<table>
<tr><th>項目</th><th colspan="2">説明</th></tr>
<tr><td>コミュニティ名</td><td colspan="2">SNMP マネージャが read 権限でアクセスするためのコミュニティ名を設定します。1 文字から 15 文字まで設定できます。write 権限でアクセスすることは出来ません。デフォルトは public です。</td></tr>
<tr><td rowspan="5">マネージャ IP アドレス[n]</td><td colspan="2">アクセスを許可する SNMP マネージャを IP アドレスとネットワーク空間で 2 つまで設定することができます。SNMP マネージャ連携を有効にする場合には 1 つ以上のマネージャ IP アドレスを設定しなければなりません。</td></tr>
<tr><td>選択項目</td><td>設定内容</td></tr>
<tr><td>指定なし</td><td>マネージャ IP アドレスを設定しません。</td></tr>
<tr><td>IP アドレス</td><td>IPv4 アドレスを設定します。</td></tr>
<tr><td>ネットワーク空間</td><td>始点アドレスとアドレス空間を表すサブネットマスクを設定します。実際のサブネットと異なる設定もできます。接続可能なアドレスに始点アドレスと終点アドレスも含まれます。</td></tr>
<tr><td>システム設置場所</td><td colspan="2">SNMP マネージャが機器の設置場所(SNMPv2-MIB::sysLocation)を問い合わせた際に使われます。デフォルトは空白です。</td></tr>
<tr><td>システム管理責任者</td><td colspan="2">SNMP マネージャが機器の管理責任者(SNMPv2-MIB::sysContact)を問い合わせた際に使われます。デフォルトは空白です。</td></tr>
</table>

管理者設定

管理者設定では iBAQS を管理するに当たり必要な情報を設定します。

- インフォメーション

  操作の概要を表示します。

- 設定状況

項目	説明
管理者 ID	管理画面へログインするためのユーザーID を設定します。1 文字から 20 文字まで設定できます。デフォルトは manager です。
管理者パスワード	管理者 ID でログインするためのパスワードを設定します。ポップアップダイアログでパスワードを入力します。6 文字から 20 文字まで設定できます。デフォルトは friend です。
管理者メールアドレス	システム設定で選択したアラートメールを送信する宛先を設定します。PC 用、携帯電話用のフォーマットが用意されています。","（カンマ）を用いて複数のアドレスにメールを送信することができます。PC 用、携帯電話用ともに 250 文字まで設定できます。デフォルトは空白です。

項目	説明	
SMTP サーバ	アラートメールを送信する際に利用する SMTP サーバを設定します。IPv4 アドレスまたは FQDN で設定します。デフォルトは空白です。	
メール認証	送信の際に手続きの必要な SMTP サーバを利用する場合に設定します。SMTP 認証と POP before SMTP をサポートします。デフォルトはなしです。	
	利用	動作
	なし	iBAQS から無条件でリレー可能な SMTP サーバを設定してください。
	SMTP 認証	メールを送信する前に認証を受けます。ユーザーID、パスワードを設定してください。
	POP before SMTP	POP サーバで認証を受けた後にメールの送信を行います。ユーザーID、パスワード、POP サーバを設定してください。
アクセス制御	管理者としてログイン可能なネットワークを限定する場合に設定します。IP アドレス、ネットワーク空間は 3 つまで設定できます。デフォルトはしないです。	
		動作
	する	アクセス制御ネットワーク 1～3 で指定したネットワーク以外からの管理者ログインを制限します。
	しない	管理者ログインを制限しません。
アクセス制御ネットワーク[n]	管理者ログインを許可するネットワークを IP アドレスとネットワーク空間で 3 つまで設定することができます。アクセス制御を有効にする場合は 1 つ以上のアクセス制御ネットワークを設定しなければなりません。	
	選択項目	設定内容
	指定なし	アクセス制御ネットワークを設定しません。
	IP アドレス	IPv4 アドレスを設定します。
	ネットワーク空間	始点アドレスとアドレス空間を表すサブネットマスクを設定します。実際のサブネットと異なる設定もできます。接続可能なアドレスに始点アドレスと終点アドレスも含まれます。

証明書設定

証明書設定ではプライベート認証局の設定、クライアント証明書の発行、ダウンロードを行います。

- インフォメーション

  プライベート認証局の状態を表示します。

- 認証局

項目	説明
ステータス	認証局の状態を設定済、未設定で表示します。
作成日時	認証局が作成された日時を表示します。
認証局名	認証局の認証局名（証明書のサブジェクト CN）を表示します。
国名	認証局の国名（証明書のサブジェクト C）を表示します。
都道府県名	認証局の都道府県名（証明書のサブジェクト S）を表示します。
市区町村名	認証局の市区町村名（証明書のサブジェクト L）を表示します。
組織名	認証局の組織名（証明書のサブジェクト O）を表示します。
部署名	認証局の（証明書のサブジェクト OU）を表示します。

項目	説明
署名アルゴリズム	認証局の署名アルゴリズムを表示します。
有効期限	認証局証明書の有効期限を表示します。

- クライアント証明書

  クライアント証明書の発行／失効、クライアント証明書のダウンロード画面へ移動できます。

認証局編集

認証局編集ではプライベート認証局の作成/更新を行います。認証局を更新する場合、既に発行している認証局証明書やクライアント証明書は使用できなくなりますのでご注意ください。

- インフォメーション

  認証局編集にあたって注意していただきたい事項が表示されます。

- 認証局

項目	説明
認証局名	認証局の認証局名（証明書のサブジェクト CN）を設定します。1 文字から 100 文字まで設定できます。必須入力です。デフォルトは空白です。
国名	認証局の国名（証明書のサブジェクト C）で JP（日本）固定です。
都道府県名	認証局の都道府県名（証明書のサブジェクト S）を設定します。1 文字から 50 文字まで設定できます。必須入力です。デフォルトは空白です。
市区町村名	認証局の市区町村名（証明書のサブジェクト L）を設定します。1 文字から 50 文字まで設定できます。必須入力です。デフォルトは空白です。

項目	説明
組織名	認証局の組織名（証明書のサブジェクト O）を設定します。1 文字から 50 文字まで設定できます。必須入力です。デフォルトは空白です。
部署名	認証局の（証明書のサブジェクト OU）を設定します。1 文字から 50 文字まで設定できます。任意入力です。デフォルトは空白です。
署名アルゴリズム	認証局の署名アルゴリズムを設定します。MD5 と SHA1 から選択できます。デフォルトは MD5 です。
有効期限	認証局証明書の有効期限を設定します。5 年から 25 年まで 5 年刻みで設定できます。証明書の有効期限が切れると発行した全ての証明書が無効となり、再発行、再配布が必要になりますので長い期間を設定することをお奨めします。デフォルトは 25 年です。

クライアント証明書発行

クライアント証明書発行では認証にクライアント証明書を選択しているクライアントの証明書を発行したり失効したりできます。

- インフォメーション

  認証にクライアント証明書を選択しているクライアントの数を表示します。

- 検索条件

項目	説明	
発行状態	クライアント証明書の発行状態により絞り込みができます。デフォルトは指定なしです。	
	選択項目	動作
	指定なし	未発行、発行済ともに表示します。
	未発行	クライアント証明書を発行していないクライアントのみを表示します。まとめて発行を行う場合にご利用ください。
	発行済	クライアント証明書を発行しているクライアントのみを表示します。まとめて失効を行う場合にご利用ください。

- 検索結果

<table>
<tr><th>項目</th><th colspan="3">説明</th></tr>
<tr><td>利用者名</td><td colspan="3">該当クライアントの利用者名を表示します。</td></tr>
<tr><td>PC 名</td><td colspan="3">該当クライアントの PC 名を表示します。</td></tr>
<tr><td>ユーザーID</td><td colspan="3">該当クライアントの認証用ユーザーID を表示します。ユーザーID はクライアント証明書のユーザーID（証明書のサブジェクト CN）に設定されます。</td></tr>
<tr><td rowspan="3">発行状態/詳細</td><td colspan="3">該当クライアントのクライアント証明書発行状態を確認できます。</td></tr>
<tr><td>発行状態</td><td>詳細</td><td>意味</td></tr>
<tr><td>未発行</td><td>未発行です。</td><td>クライアント証明書は発行されていません。発行にチェックを入れて証明書発行を行ってください。</td></tr>
<tr><td>発行済</td><td>発行済です。</td><td>クライアント証明書は既に発行されています。失効の必要がある場合には失効にチェックを入れて証明書失効を行ってください。</td></tr>
<tr><td>発行</td><td colspan="3">クライアント証明書が未発行の場合のみチェックボックスを表示します。チェックして画面下部にあるクライアント証明書発行ボタンをクリックするとチェックしたクライアントの証明書が発行されます。発行した証明書は証明書設定画面下部にあるクライアント証明書のダウンロードへのリンクをクリックしてダウンロードを行ってください。</td></tr>
<tr><td>失効</td><td colspan="3">クライアント証明書が発行済の場合のみチェックボックスを表示します。チェックして画面下部にあるクライアント証明書失効ボタンをクリックするとチェックしたクライアントの証明書が失効されます。失効した証明書は認証に使用できなくなります。再発行した際にはサブジェクトは同一でも異なる証明書が発行されますので注意して失効を行ってください。</td></tr>
</table>

クライアント証明書ダウンロード

クライアント証明書ダウンロードでは発行済のクライアント証明書をダウンロードできます。

- インフォメーション

  発行済クライアント証明書の件数を表示します。

- クライアント証明書

項目	説明
利用者名	該当クライアントの利用者名を表示します。
PC 名	該当クライアントの PC 名を表示します。
ユーザーID	該当クライアントの認証用ユーザーID を表示します。ユーザーID はクライアント証明書のユーザーID（証明書のサブジェクト CN）に設定されています。
有効期限	発行したクライアント証明書の有効期限を表示します。有効期限の切れた証明書は認証に使用できませんのでご注意ください。
ダウンロード	発行したクライアント証明書をダウンロードするにはチェックボックスにチェックを入れ、画面下部のクライアント証明書ダウンロードボタンをクリックします。形式は PKCS#12、PEM の 2 種類で、client_cert.zip という名前の圧縮ファイルとなってダウンロードします。ファイル名とユーザーID が同一となっておりますので、それぞれを該当するクライアントにインポートしてください。なお、証明書による認証を行う場合、コンピュータアカウントに対しても証明書のインポートを行い、ログオン前認証が実施できるように設定ください。ログオン前認証が有効になっていない場合、AVS 確認が正常に行われません。

DHCP 設定

DHCP 設定では DHCP サーバの設定をします。基本タブは全セグメント共通の設定項目となります。セグメントタブの一番上に表示される iBAQS の所属するセグメントはシステムの動作に必要なので削除できません。

- インフォメーション

  現在登録されているセグメント数を表示します。

- 設定状況

項目	説明
リース時間	DHCP サーバがクライアントに払い出す IP アドレスのリース時間を設定します。セグメント毎にも設定可能で、セグメントに設定した値が優先されます。1 分から 6 日 23 時間 59 分まで設定できます。デフォルトは 1 日です。
DNS	DHCP サーバがクライアントに払い出す DNS、WINS サーバの情報を設定します。セグメント毎にも設定可能で、セグメントに設定した値が優先されます。Primary、Secondary を空白に設定し、Tertiary に値を入れた場合、設定後は Primary に反映されます。デフォルトは空白です。
WINS	

項目	説明
セグメント名	セグメントの名前を表示します。
ネットワーク	セグメントのネットワークアドレスを表示します。
サブネット	セグメントのサブネットマスクを表示します。
ゲートウェイ	セグメントのデフォルトゲートウェイを表示します。
編集	アイコン をクリックすると該当セグメントの編集を行うことができます。
削除	アイコン をクリックすると該当セグメントの削除を行うことができます。

セグメント追加

セグメント追加では DHCP サーバで扱うネットワークの追加を行います。追加を行ったネットワークからの DHCP 要求が iBAQS にリレーされるようにルータ、L3 スイッチ等を適切に設定してください。

- インフォメーション

  操作の概要を表示します。

- 設定状況

項目	説明
セグメント名	セグメントの名前を設定します。1 文字から 30 文字まで設定できます。全角文字も 1 字で数えます。
ネットワークアドレス	セグメントのネットワークアドレスを設定します。他のセグメントと重なるネットワークは設定できません。
サブネットマスク	セグメントのサブネットマスクを設定します。
デフォルトゲートウェイ	セグメントのデフォルトゲートウェイを設定します。セグメントのネットワーク範囲外のアドレスは指定できません。DHCP サーバからクライアントにデフォルトゲートウェイのアドレスとして渡されます。デフォルトは空白です。

項目	説明
リース時間	セグメント単位でリース時間を変更する場合には設定します。1 分から 6 日 23 時間 59 分まで設定できます。デフォルトは空白で、システム設定のデフォルトリース時間が有効です。
DNS	セグメント単位で別の DNS サーバの情報をクライアントに渡す場合にはセグメント DNS を設定します。設定覧の右にシステム設定のデフォルト DNS を表示します。セグメント DNS を 1 つでも設定するとデフォルト DNS は継承されなくなるのでご注意ください。
WINS	セグメント単位で別の WINS サーバの情報をクライアントに渡す場合にはセグメント WINS を設定します。設定覧の右にシステム設定のデフォルト WINS を表示します。セグメント WINS を 1 つでも設定するとデフォルト WINS は継承されなくなるのでご注意ください。

セグメント編集

セグメント編集では登録済のセグメント情報を更新します。

- インフォメーション

  操作の概要を表示します。

- 設定状況

項目	説明
セグメント名	セグメントの名前を設定します。1 文字から 30 文字まで設定できます。全角文字も 1 字で数えます。
ネットワークアドレス	セグメントのネットワークアドレスを設定します。他のセグメントと重なるネットワークは設定できません。サーバセグメントと同一のセグメントは変更できません。サーバ設定から変更してください。
サブネットマスク	セグメントのサブネットマスクを設定します。サーバセグメントと同一のセグメントは変更できません。サーバ設定から変更してください。

項目	説明
デフォルトゲートウェイ	セグメントのデフォルトゲートウェイを設定します。セグメントのネットワーク範囲外のアドレスは指定できません。DHCP サーバからクライアントにデフォルトゲートウェイのアドレスとして渡されます。デフォルトは空白です。サーバセグメントと同一のセグメントは変更できません。サーバ設定から変更してください。
リース時間	セグメント単位でリース時間を変更する場合には設定します。1 分から 6 日 23 時間 59 分まで設定できます。デフォルトは空白で、システム設定のデフォルトリース時間が有効です。
DNS	セグメント単位で別の DNS サーバの情報をクライアントに渡す場合にはセグメント DNS を設定します。設定覧の右にシステム設定のデフォルト DNS を表示します。セグメント DNS を 1 つでも設定するとデフォルト DNS は継承されなくなるのでご注意ください。
WINS	セグメント単位で別の WINS サーバの情報をクライアントに渡す場合にはセグメント WINS を設定します。設定覧の右にシステム設定のデフォルト WINS を表示します。セグメント WINS を 1 つでも設定するとデフォルト WINS は継承されなくなるのでご注意ください。

セグメント削除

セグメント削除では登録済のセグメントを削除します。

- インフォメーション

  セグメント削除に当たっての注意事項を表示します。

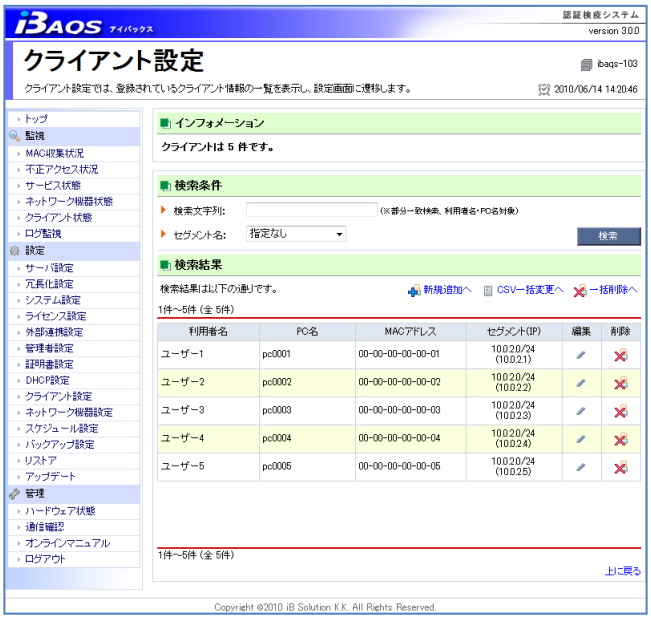
- 設定状況

  削除するセグメントの情報を表示します。間違いがなければ削除ボタンで削除を実行してください。

項目	説明
セグメント名	セグメントの名前を表示します。
ネットワークアドレス	セグメントのネットワークアドレスを表示します。
サブネットマスク	セグメントのサブネットマスクをひょじします。
デフォルトゲートウェイ	セグメントのデフォルトゲートウェイを表示します。
リース時間	セグメントのリース時間を表示します。
DNS	セグメントの DNS 払い出し情報を表示します。
WINS	セグメントの WINS 払い出し情報を表示します。

クライアント設定

クライアント設定では登録されているクライアントの確認、新規追加、編集、一括変更、削除、一括削除を行えます。



- インフォメーション

  現在登録されているクライアント数が表示されます。

- 検索条件

項目	説明
検索文字列	利用者名、PC 名から指定した文字列を含むクライアントを検索します。デフォルトは空白で絞り込みを行いません。 半角全角問わず最大 50 文字まで指定可能で、部分一致検索です。 長い文字列を入力した場合には全体を表示できない場合がありますので、カーソルキー等を利用してスクロールしてください。
セグメント名	クライアントの所属するセグメントによって絞り込むことができます。指定なしおよび登録されているセグメント名を設定できます。デフォルトは指定なしです。

- 検索結果

項目	説明
利用者名	該当クライアントの利用者名を表示します。
PC 名	該当クライアントの PC 名を表示します。
MAC アドレス	該当クライアントの MAC アドレスを表示します。
セグメント(IP)	該当クライアントの所属セグメントおよび IP アドレスを表示します。複数のセグメントに所属している場合には複数行表示します。
編集	アイコン をクリックすると該当クライアントの編集を行うことができます。
削除	アイコン をクリックすると該当クライアントの削除を行うことができます。

クライアント追加

クライアント追加ではネットワークを利用するクライアントの追加を行います。

- インフォメーション

  操作の概要を表示します。

- 設定状況

項目	説明
利用者名	クライアントの利用者名を設定します。
PC 名	クライアントの PC 名を設定します。
所属セグメント	クライアントの所属するセグメントと IP アドレスを設定します。クライアントは DHCP に設定してください。設定変更が難しい場合にはクライアントに設定している IP アドレスと同一の IP アドレスを設定してください。 右上にあるセグメント追加ボタンをクリックすると最大 10 個まで所属セグメントを追加することができます。

項目	説明	
MAC アドレス	クライアントの MAC アドレスを設定します。認証や IP アドレスの払い出し、通信制限に使用されますので間違いなく設定してください。	
認証	認証に使用する項目を設定します。AVS 確認の要件でログイン前にもネットワークに接続する必要があるため、ユーザーID を選択した場合にはログオン前認証を利用可能なサプリカントを別途ご用意ください。Windows 標準サプリカントではログオン前認証を利用できません。	
	設定値	意味
	MAC アドレス	MAC ベース認証を使用します。必須で対象から外すことは出来ません。
	ユーザーID	EAP-MD5、PEAP 認証に使用します。MAC アドレスを評価しますので、異なるクライアントからの認証に使用できません。
	クライアント証明書	EAP-TLS 認証を使用します。クライアント証明書は証明書設定から発行、ダウンロードできます。通常の EAP-TLS 認証と異なり、MAC アドレスを評価するので、異なるクライアントからの認証には使用できません。認証局証明書、クライアント証明書はユーザーアカウント、コンピュータアカウント双方に登録してください。
認証ユーザーID	EAP-MD5、PEAP で使用するユーザーID、EAP-TLS で使用する証明書のユーザーID（証明書のサブジェクト CN）を設定します。MAC ベース認証のみを使用する場合には設定不要です。	
認証パスワード	EAP-MD5、PEAP で使用するパスワード、EAP-TLS で使用する証明書のパスワードを設定します。MAC ベース認証のみを使用する場合には設定不要です。	
クライアント証明書 有効期間	クライアント証明書を使用する場合に設定します。1 年、2 年、3 年、4 年、5 年、10 年、15 年、20 年から設定します。デフォルトは 1 年です。一度クライアント証明書を発行してしまうと延長はできませんので注意して設定してください。	
アンチウイルスソフト確認	AVS の動作確認対象であれば「する」を、Windows 以外の PC、ネットワークプリンタ等であれば「しない」を設定します。Windows の PC でも AVS 確認を必要としない場合には「しない」を設定してください。「する」を選択した場合には認証を受けた後で接続したネットワーク機器に通信制限が適用され、AVS 確認が完了した時点で通信制限が解除されます。	

クライアント利用	クライアントの一時利用停止を行いたい場合に「しない」に設定します。クライアント証明書を利用するクライアントでは証明書の失効を伴わずにネットワーク接続を禁止することができます。即時反映されます。
認証有効期限	クライアントの認証可能な期間を設定します。有効期限が切れるとクライアント状態監視処理によりネットワーク接続が禁止されます。
VLAN 制御	ダイナミック VLAN を使用する場合には「する」を選択し、VLAN ID を入力します。VLAN ID は 1 から 4094 まで設定できます。デフォルトは「しない」です。
メールアドレス	パスワード期限切れ（利用者）のアラートメールを使用する場合に設定します。クライアント状態監視処理により使用します。
備考	クライアントに関するメモ等にご利用ください。設定内容が動作に影響を及ぼすことはありません。

クライアント一括変更

クライアント一括変更では CSV ファイルを用いたクライアントの一括登録、一括変更、一括削除を行うことができます。また、現在登録されているクライアントを一括変更で使用する形式の CSV ファイルでダウンロードできます。

- インフォメーション

  操作の概要を表示します。

- クライアント インポート

  クライアントの一括変更を行う場合には、参照ボタンをクリックして一括変更に使用する CSV ファイルを選択し、インポートボタンをクリックします。

- CSV ファイルの書式

CSV ファイルは以下の 40 項目で構成されます。
[制御文字]、[クライアント CD]、[利用者名]、[PC 名]、[認証対象]、[MAC アドレス]、
[ユーザーID 認証]、[クライアント証明書認証]、[認証ユーザーID]、
[認証パスワード]、[クライアント証明書有効期間]、[アンチウイルスソフト確認]、
[クライアント利用]、[認証有効期限制御]、[認証有効期限]、[VLAN 制御]、[VLAN ID]、
[メールアドレス]、[備考]、[セグメント名 1]、[IP アドレス 1]、[セグメント名 2]、
[IP アドレス 2]、[セグメント名 3]、[IP アドレス 3]、[セグメント名 4]、
[IP アドレス 4]、[セグメント名 5]、[IP アドレス 5]、[セグメント名 6]、
[IP アドレス 6]、[セグメント名 7]、[IP アドレス 7]、[セグメント名 8]、
[IP アドレス 8]、[セグメント名 9]、[IP アドレス 9]、[セグメント名 10]、
[IP アドレス 10]、[終端文字]

例 1. 追加の場合
A,,福井太郎,pc-fukui,00-00-00-00-00-00-01,0,0,,,,1,1,0,,0,,tarou@ibaqs.local,
〇〇担当,デフォルトセグメント,192.168.1.100,,,,,,,,,,,,,,,,,,E

例 2. 編集の場合
U,33, 福井太郎,pc-fukui,00-AA-AA-AA-AA-AA-AA,0,0,,,,1,1,0,,0,,
tarou@ibaqs.co.jp, △△担当,デフォルトセグメント,192.168.1.100,
セグメント２,192.168.2.100,,,,,,,,,,,,,,,,E
※クライアント CD は、「クライアントエクスポート」を利用することで取得できます。

例 3. 削除の場合
D,33,,,E
※クライアント CD は、「クライアントエクスポート」を利用することで取得できます。

項目	説明
制御文字	処理内容を設定します。 追加の場合・・・「A」 編集の場合・・・「U」 削除の場合・・・「D」 上記以外の文字の場合、処理されません。

項目	説明
クライアント CD	クライアントコードを設定します。 クライアントコードは登録済みのクライアントの付加情報で、「クライアントエクスポート」を利用することで取得できます。 編集／削除を行う場合は必須入力です。
利用者名	利用者名を設定します。 1 文字から 50 文字まで設定できます。全角文字も 1 字として数えます。
PC 名	PC 名を設定します。 1 文字から 50 文字まで設定できます。半角英数字と"-"（ハイフン）、"_"（アンダーバー）が利用できます。
認証対象	認証対象を入力します。 MAC アドレス・・・「0」 MAC アドレス/ユーザーID・・・「1」 MAC アドレス/クライアント証明書・・・「2」 MAC アドレス/ユーザーID/クライアント証明書・・・「3」
MAC アドレス	MAC アドレスを設定します。 "-"（ハイフン）区切りの半角英数字で設定します。
ユーザーID 認証	ユーザーID での認証使用可否を設定します。 する場合・・・「1」 しない場合・・・「0」 半角数字の 0 か 1 設定します。
クライアント証明書認証	クライアント証明書での認証使用可否を設定します。 する場合・・・「1」 しない場合・・・「0」 半角数字の 0 か 1 設定します。
認証ユーザーID	ユーザーID 認証およびクライアント証明書認証で利用するユーザーID を設定します。 ユーザーID 認証またはクライアント証明書認証を使用する場合、必須入力です。
認証パスワード	ユーザーID 認証およびクライアント証明書認証で利用するパスワードを設定します。 ユーザーID 認証またはクライアント証明書認証を使用する場合、必須入力です。

項目	説明
クライアント証明書有効期間	クライアント証明書認証で利用するクライアント証明書の有効期間を設定します。 1 年・・・「1」 2 年・・・「2」 3 年・・・「3」 4 年・・・「4」 5 年・・・「5」 10 年・・・「10」 15 年・・・「15」 20 年・・・「20」 半角数字で上記数字を設定します。クライアント証明書認証を使用する場合、必須入力です。
アンチウイルスソフト確認	アンチウイルスソフト確認使用可否を設定します。 する場合・・・「1」 しない場合・・・「0」 半角数字の 0 か 1 を設定します。
クライアント利用	クライアント利用可否を設定します。 する場合・・・「1」 しない場合・・・「0」 半角数字の 0 か 1 を設定します。
認証有効期限制御	認証有効期限使用可否を設定します。 する場合・・・「1」 しない場合・・・「0」 半角数字の 0 か 1 を設定します。
認証有効期限	認証有効期限を設定します。 入力形式は、YYYY/MM/DD で、未来日を入力します。 認証有効期限を使用する場合、必須入力です。
VLAN 制御	認証有効期限使用可否を設定します。 する場合・・・「1」 しない場合・・・「0」 半角数字の 0 か 1 を設定します。
VLAN ID	VLAN 制御で使用する VLAN ID を設定します。 半角数字で 1 から 4094 で入力します。 VLAN 制御を利用する場合、必須入力です。

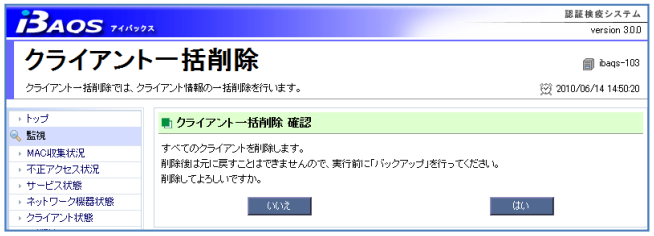
項目	説明
メールアドレス	メールアドレスを設定します。 値の入力は任意です。
備考	備考を設定します。 値の入力は任意です。
セグメント名 1	セグメント名を設定します。 入力するセグメント名は登録済のセグメント名です。 処理内容が登録と編集の場合には必須入力です。
IP アドレス 1	IP アドレスを設定します。 入力する IP アドレスはセグメント 1 のネットワーク範囲でなければなりません。
セグメント名 2～10	セグメント名を設定します。 入力するセグメント名は登録済のセグメント名です。 複数のセグメントに所属させる場合に必要に応じて設定します。
IP アドレス 2～10	IP アドレスを入力します。 入力する IP アドレスはセグメント 2～10 のネットワーク範囲でなければなりません。 複数のセグメントに所属させる場合に必要に応じて設定します。
終端文字	終端文字を設定します。 終端文字・・・「E」 終端文字は必須入力です。

- クライアント エクスポート

エクスポートボタンをクリックすることで、登録済のクライアントをすべてエクスポートします。
クライアント一括更新で編集や削除を行う場合にはエクスポートを利用してください。

クライアント一括削除

クライアント一括削除では登録されているすべてのクライアントを一度に削除します。念のためにバックアップを採取してから削除されることを推奨します。クライアント証明書が発行済のクライアントがある場合、一括削除は利用できません。事前に発行済のクライアント証明書をすべて失効してください。



- クライアント一括削除確認

  クライアント一括削除を行うには「はい」を、キャンセルする場合には「いいえ」をクリックします。「いいえ」をクリックした場合、クライアント設定画面に戻ります。

クライアント編集

クライアント編集では登録済クライアントの編集を行うことができます。

- インフォメーション

  操作の概要を表示します。

- 設定状況

項目	説明
利用者名	クライアントの利用者名を設定します。
PC 名	クライアントの PC 名を設定します。
所属セグメント	クライアントの所属するセグメントと IP アドレスを設定します。クライアントは DHCP に設定してください。設定変更が難しい場合にはクライアントに設定している IP アドレスと同一の IP アドレスを設定してください。 右上にあるセグメント追加ボタンをクリックすると最大 10 個まで所属セグメントを追加することができます。

項目	説明	
MAC アドレス	クライアントの MAC アドレスを設定します。認証や IP アドレスの払い出し、通信制限に使用されますので間違いなく設定してください。	
認証	認証に使用する項目を設定します。AVS 確認の要件でログイン前にもネットワークに接続する必要があるため、ユーザーID を選択した場合にはログオン前認証を利用可能なサプリカントを別途ご用意ください。Windows 標準サプリカントではログオン前認証を利用できません。	
	設定値	意味
	MAC アドレス	MAC ベース認証を使用します。必須で対象から外すことは出来ません。
	ユーザーID	EAP-MD5、PEAP 認証に使用します。MAC アドレスを評価しますので、異なるクライアントからの認証に使用できません。
	クライアント証明書	EAP-TLS 認証を使用します。クライアント証明書は証明書設定から発行、ダウンロードできます。通常の EAP-TLS 認証と異なり、MAC アドレスを評価するので、異なるクライアントからの認証には使用できません。認証局証明書、クライアント証明書はユーザーアカウント、コンピュータアカウント双方に登録してください。
認証ユーザーID	EAP-MD5、PEAP で使用するユーザーID、EAP-TLS で使用する証明書のユーザーID（証明書のサブジェクト CN）を設定します。MAC ベース認証のみを使用する場合には設定不要です。クライアント証明書を発行済の場合には変更できません。	
認証パスワード	EAP-MD5、PEAP で使用するパスワード、EAP-TLS で使用する証明書のパスワードを設定します。MAC ベース認証のみを使用する場合には設定不要です。クライアント証明書を発行済の場合には変更できません。	
クライアント証明書有効期間	クライアント証明書を使用する場合に設定します。1 年、2 年、3 年、4 年、5 年、10 年、15 年、20 年から設定します。デフォルトは 1 年です。一度クライアント証明書を発行してしまうと延長はできませんので注意して設定してください。クライアント証明書を発行済の場合には変更できません。	

項目	説明
アンチウイルスソフト確認	AVS の動作確認対象であれば「する」を、Windows 以外の PC、ネットワークプリンタ等であれば「しない」を設定します。Windows の PC でも AVS 確認を必要としない場合には「しない」を設定してください。「する」を選択した場合には認証を受けた後で接続したネットワーク機器に通信制限が適用され、AVS 確認が完了した時点で通信制限が解除されます。
クライアント利用	クライアントの一時利用停止を行いたい場合に「しない」に設定します。クライアント証明書を利用するクライアントでは証明書の失効を伴わずにネットワーク接続を禁止することができます。即時反映されます。
認証有効期限	クライアントの認証可能な期間を設定します。有効期限が切れるとクライアント状態監視処理によりネットワーク接続が禁止されます。
VLAN 制御	ダイナミック VLAN を使用する場合には「する」を選択し、VLAN ID を入力します。VLAN ID は 1 から 4094 まで設定できます。デフォルトは「しない」です。
メールアドレス	パスワード期限切れ（利用者）のアラートメールを使用する場合に設定します。クライアント状態監視処理により使用します。
備考	クライアントに関するメモ等にご利用ください。設定内容が動作に影響を及ぼすことはありません。
パスワード更新日	パスワード更新日を表示します。
登録日	クライアントを登録した日を表示します。

クライアント削除

クライアント削除ではクライアントの削除を行えます。

- インフォメーション

  操作に関する概要を表示します。

- 設定状況

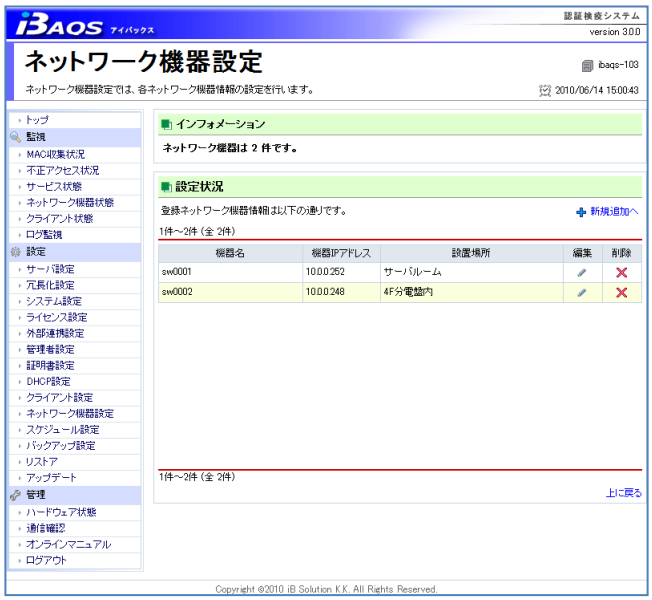
  削除対象の情報を表示します。間違いがなければ削除ボタンで削除してください。

項目	説明
利用者名	クライアントの利用者名を表示します。
PC 名	クライアントの PC 名を表示します。
所属セグメント	クライアントの所属するセグメントと IP アドレスを表示ます。

項目	説明	
認証	認証に使用する項目を表示します。	
	設定値	意味
	MAC アドレス	MAC アドレスを表示します。
	ユーザーID	ユーザーID 認証の使用可否を表示します。
	クライアント証明書	クライアント証明書認証の使用可否を表示します。
認証ユーザーID	認証に使用するユーザーID を表示します。	
クライアント証明書有効期間	クライアント証明書の有効期間を表示します。	
クライアント証明書発行状態	クライアント証明書の発行状態を「発行済」、「未発行」で表示します。 「発行済」の場合にはクライアントを削除できません。	
クライアント利用	クライアント利用の状態を表示します。	
認証有効期限制御	認証有効期限の状態を表示します。期限が設定されている場合には有効期限も表示します。	
VLAN 制御	VLAN 制御の状態を表示します。	
メールアドレス	メールアドレスを表示します。	
備考	備考に入力されたメモ等を表示します。	
パスワード更新日	パスワード更新日を表示します。	
登録日	クライアントを登録した日を表示します。	

ネットワーク機器設定

ネットワーク機器設定では登録済ネットワーク機器の確認、追加、編集、削除を行えます。



- インフォメーション

  現在登録されているネットワーク機器の台数を表示します。

- 設定状況

  現在の登録状況を表示します。

項目	説明
機器名	ネットワーク機器名を表示します。
機器 IP アドレス	ネットワーク機器の IP アドレスを表示します。
設置場所	ネットワーク機器の設置場所を表示します。
編集	アイコン をクリックすると該当ネットワーク機器の編集を行うことができます。
削除	アイコン をクリックすると該当ネットワーク機器の削除を行うことができます。

ネットワーク機器追加

ネットワーク機器追加では認証、通信制限に使用するネットワーク機器を設定します。

- インフォメーション

  操作の概要を表示します。

- 設定状況

項目	説明
機器名	機器名を設定します。最大 32 文字まで設定可能です。
機器種別	リストボックスから機器を選択します。機器を誤って選択すると telnet での制御が正常に行われませんのでご注意ください。
機器 IP アドレス	ネットワーク機器の IP アドレスを設定します。IP アドレスを誤って設定すると認証、制御が正常に行われませんのでご注意ください。
設置場所	ネットワーク機器の設置場所を設定します。不正アクセスやネットワーク機器異常のアラートメールに使用します。1 文字から 50 文字まで設定できます。全角も 1 字で計算します。
ログイン ID	telnet で制御する際のログイン ID を設定します。
ログインパスワード	telnet で制御する際のログインパスワードを設定します。設定ボタンをクリックし、ポップアップウィンドウでパスワードを設定します。6 文字から 20 文字まで設定できます。
フィルタ番号	選択する機器によって必須入力となります。通信制限用のフィルタを定義する際に使用します。詳しくは設定例をご確認ください。 ※ 追加後にはAVS を未導入または停止したクライアントを接続して正しく隔離されることを確認してください。
共有パスワード	RADIUS 認証で使用する共有パスワードを設定します。設定ボタンをクリックし、ポップアップウィンドウでパスワードを設定します。6 文字から 20 文字まで設定できます。
購入日（西暦）	ネットワーク機器の購入日を設定します。任意入力です。

ネットワーク機器編集

ネットワーク機器編集では既に登録されているネット枠機器の情報を変更します。

- インフォメーション

  操作の概要を表示します。

- 設定状況

項目	説明
機器名	機器名を設定します。最大 32 文字まで設定可能です。
機器種別	リストボックスから機器を選択します。機器を誤って選択すると telnet での制御が正常に行われませんのでご注意ください。
機器 IP アドレス	ネットワーク機器の IP アドレスを設定します。IP アドレスを誤って設定すると認証、制御が正常に行われませんのでご注意ください。
設置場所	ネットワーク機器の設置場所を設定します。不正アクセスやネットワーク機器異常のアラートメールに使用します。1 文字から 50 文字まで設定できます。全角も 1 字で計算します。
ログイン ID	telnet で制御する際のログイン ID を設定します。
ログインパスワード	telnet で制御する際のログインパスワードを設定します。設定ボタンをクリックし、ポップアップウィンドウでパスワードを設定します。6 文字から 20 文字まで設定できます。
フィルタ番号	選択する機器によって必須入力となります。通信制限用のフィルタを定義する際に使用します。詳しくは設定例をご確認ください。 ※ 変更後にはAVS を未導入または停止したクライアントを接続して正しく隔離されることを確認してください。
共有パスワード	RADIUS 認証で使用する共有パスワードを設定します。設定ボタンをクリックし、ポップアップウィンドウでパスワードを設定します。6 文字から 20 文字まで設定できます。
購入日（西暦）	ネットワーク機器の購入日を設定します。任意入力です。

ネットワーク機器削除

ネットワーク機器削除では登録済のネットワーク機器を削除します。
削除を行うと、認証、通信制限の解除が行われなくなりますのでご注意ください。

- インフォメーション

  削除に当たっての注意事項を表示します。

- 設定状況

  設定内容を確認の上、問題がなければ削除ボタンをクリックして削除を実行してください。

項目	説明
機器名	ネットワーク機器の機器名を表示します。
機器 IP アドレス	ネットワーク機器の IP アドレスを表示します。
設置場所	ネットワーク機器の設置場所を表示します。
ログイン ID	telnet で制御する際のログイン ID を表示します。
フィルタ番号	通信制限用のフィルタ番号を表示します。
購入日（西暦）	ネットワーク機器の購入日を表示します。

スケジュール設定

スケジュール設定では定期的に実行するバッチジョブの実行状態、実行周期を設定できます。

- インフォメーション

  操作の概要を表示します。

- スケジュール設定

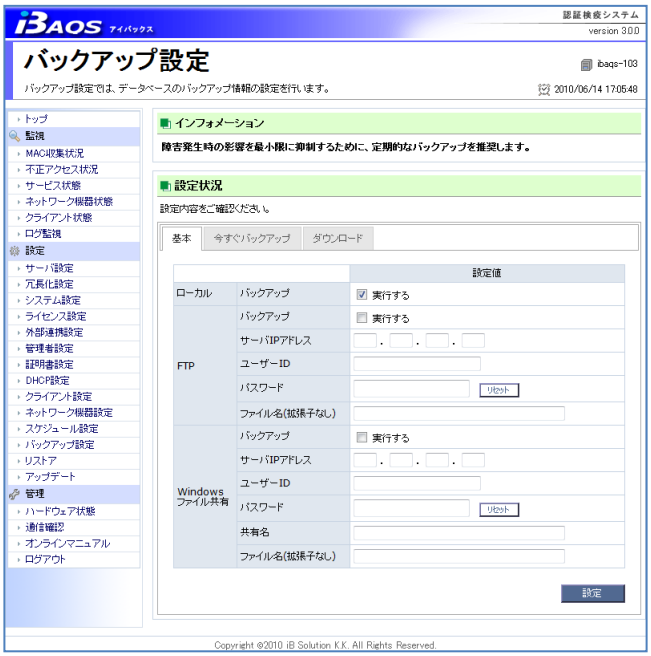
項目	説明		
バックアップ処理	バックアップ設定で設定した内容で設定情報をバックアップします。 自動実行は無効にできます。実行周期は毎日、毎週（曜日指定）、毎月（1-27、月末）です。開始時刻は時、分で設定します。バックアップ処理時、認証パフォーマンスが若干低下しますので業務時間外に実行するように調整してください。		
	状況	詳細	説明
	有効	毎日 N 時 N 分	毎日設定した時刻に処理を開始します。
		毎週 X 曜日 N 時 N 分	毎週設定した曜日、時刻に処理を開始します。
		毎月 N 日 N 時 N 分	毎月設定した日、時刻に処理を開始します。
	無効	-	処理は無効です。

<table>
<tr><th>項目</th><th colspan="3">説明</th></tr>
<tr><td>データベース不要領域復旧処理</td><td colspan="3">ログ削除処理により使用されなくなったデータベースの領域を開放し再利用可能にします。これによりデータベースのサイズが大きくなることを防ぎます。ログ削除処理の 30 分から 1 時間後に実行すると効果的です。データベース不要領域復旧処理時、認証パフォーマンスが若干低下しますので業務時間外に実行するように調整してください。</td></tr>
<tr><td></td><td>状況</td><td>詳細</td><td>説明</td></tr>
<tr><td></td><td>有効</td><td>毎日 N 時 N 分</td><td>毎日設定した時刻に処理を開始します。</td></tr>
<tr><td></td><td></td><td>毎週 X 曜日 N 時 N 分</td><td>毎週設定した曜日、時刻に処理を開始します。</td></tr>
<tr><td></td><td></td><td>毎月 N 日 N 時 N 分</td><td>毎月設定した日、時刻に処理を開始します。</td></tr>
<tr><td>サービス監視処理</td><td colspan="3">サービスの稼働状況を定期的に確認します。システム設定のアラートメールでシステム異常時を選択している場合にサービス停止を検出すると管理者へアラートメールを送信します。</td></tr>
<tr><td></td><td>状況</td><td>詳細</td><td>説明</td></tr>
<tr><td></td><td>有効</td><td>毎 N 分</td><td>設定した分周期で処理を開始します。</td></tr>
<tr><td></td><td>無効</td><td>-</td><td>処理は無効です。</td></tr>
<tr><td>ネットワーク機器状態監視処理</td><td colspan="3">登録されているネットワーク機器の死活監視を行います。監視は各機器 1 回の ping で行います。タイムアウト値は 1 秒です。オンデマンド VPN で常時通信できない拠点にネットワーク機器が設置されている場合には無効にすることをお奨めします。</td></tr>
<tr><td></td><td>状況</td><td>詳細</td><td>説明</td></tr>
<tr><td></td><td>有効</td><td>毎 N 分</td><td>設定した分周期で処理を開始します。</td></tr>
<tr><td></td><td>無効</td><td>-</td><td>処理は無効です。</td></tr>
<tr><td>クライアント状態監視処理</td><td colspan="3">クライアントの認証有効期限の確認、ユーザーID 認証のパスワード有効期限確認、認証有効期限警告処理、パスワード有効期限警告処理、認証局有効期限警告処理、クライアント証明書有効期限警告処理を行います。自動実行は無効にできません。実行周期は毎日固定です。開始時刻は時、分で設定します。</td></tr>
<tr><td></td><td>状況</td><td>詳細</td><td>説明</td></tr>
<tr><td></td><td>有効</td><td>毎日 N 時 N 分</td><td>毎日設定した時刻に処理を開始します。</td></tr>
</table>

<table>
<tr><th>項目</th><th colspan="3">説明</th></tr>
<tr><td>クライアント通信監視処理</td><td colspan="3">AVS 未確認クライアント確認、AVS 未確認クライアント警告処理、AVS 停止判定処理、AVS 停止警告処理、AVS 停止時動作クライアント隔離処理を行います。AVS 停止時動作クライアントとは最終 AVS 確認から AVS 確認不要時間を超えており、最後に認証を受けたスイッチの FDB に MAC アドレスが載っているクライアントを指します。自動実行は無効にできません。</td></tr>
<tr><td></td><td>状況</td><td>詳細</td><td>説明</td></tr>
<tr><td></td><td>有効</td><td>毎 N 分</td><td>設定した分周期で処理を開始します。</td></tr>
<tr><td>アップデート確認通知処理</td><td colspan="3">アップデート確認処理、アップデート通知処理を行います。ライセンス有効期限を過ぎている場合、確認、通知ともに行われません。実行周期は毎日固定です。開始時刻は時、分で設定します。</td></tr>
<tr><td></td><td>状況</td><td>詳細</td><td>説明</td></tr>
<tr><td></td><td>有効</td><td>毎日 N 時 N 分</td><td>毎日設定した時刻に処理を開始します。</td></tr>
<tr><td></td><td>無効</td><td>-</td><td>処理は無効です。</td></tr>
</table>

バックアップ設定

バックアップ設定では設定情報のバックアップ方法を設定します。また、設定した内容での今すぐ（オンデマンド）バックアップ、ローカルバックアップファイルのダウンロードもできます。定期実行に関してはスケジュール設定のバックアップ処理で設定できます。



- インフォメーション

  設定に関する注意事項を表示します。

- 設定状況

項目	説明
ローカルバックアップ	実行するにチェックを入れると iBAQS 本体内に 1 世代のみバックアップを行います。今すぐバックアップを行うと定期バックアップのファイルが上書きされますのでご注意ください。

項目	説明	
FTP	実行するにチェックを入れると設定したFTPサーバにバックアップファイルをPUTします。	
	サーバIPアドレス	FTPサーバのIPアドレスを設定します。
	ユーザーID	FTPサーバのユーザーIDを設定します。ホームディレクトリにバックアップファイルをPUTするので、ホームディレクトリに書き込み権限のあるユーザーID を設定します。
	パスワード	FTPサーバのパスワードを設定します。設定ボタンをクリックで表示されるポップアップウインドウで設定します。
	ファイル名	FTPサーバにPUTする際のファイル名を指定します。実際に FTP サーバに PUT するファイルは[設定ファイル名].YYMMDD.tar.gz というファイル名になります。
SMB	実行するにチェックを入れると設定したWindowsファイル共有に対してバックアップファイルをコピーします。使用プロトコルはCIFSです。	
	サーバIPアドレス	Windows ファイル共有を提供するホストの IP アドレスを設定します。
	ユーザーID	共有リソースに接続するためのユーザーID を設定します。共有リソース直下にバックアップファイルをコピーするので、共有リソース直下に書き込み権限のあるユーザーIDを設定します。
	パスワード	共有リソースに接続するためのパスワードを設定します。
	マウントポイント	共有リソース名を設定します。
	ファイル名	共有リソースにコピーする際のファイル名を指定します。実際に共有リソースにコピーするファイルは[設定ファイル名].YYMMDD.tar.gz というファイル名になります。

- 今すぐバックアップ

  バックアップボタンをクリックすると現時点のバックアップを作成します。設定状況を変更した後で設定ボタンをクリックしていない場合には変更が反映されない状態でバックアップが行われますので注意してください。同日、既に定期バックアップを実行済の場合にはバックアップファイルが上書きされてしまいますので、事前にローカルバックアップファイルのダウンロード、FTP や Windows ファイル共有上のファイル待避またはリネームをお願いします。

- ダウンロード

  ダウンロードボタンをクリックすると現時点のローカルバックアップファイルをダウンロードすることができます。定期バックアップでローカルバックアップを行っていれば前回バックアップ処理実行時のバックアップファイルを、今すぐバックアップを行っていれば今すぐバックアップを行った時点でのバックアップファイルをダウンロードします。

リストア

リストアではバックアップファイルを用いた設定情報の復元を行います。また、初期設定へ戻すこともできます。リストア後は自動的に再起動が行われます。認証、AVS 確認、通信制限制御が停止しますので、運用中のリストアは行わないでください。

- インフォメーション

  操作に関する概要を表示します。

- バックアップファイルでのリストア

  バックアップファイル採取時の設定を復元します。ログ情報に関しては復元しません。リストアを行うには参照ボタンをクリックして復元するバックアップファイルを選択し、リストアボタンをクリックします。リストアには少し時間がかかります。リストア後は自動的に再起動を行います。再起動時に認証、AVS 確認、通信制限制御が停止しますので運用中のリストアは避けてください。冗長構成時に冗長構成時以外のバックアップファイルをリストアするとシステムが正しく動作しなくなりますので特別な理由がない場合には行わないようにしてください。

- 工場出荷時に戻す

  初期状態の設定を復元します。ログ情報は全て消去されますのでご注意ください。工場出荷時に戻すには工場出荷時に戻すボタンをクリックします。リストアには少し時間がかかります。リストア後は自動的に再起動を行います。

アップデート

アップデートではアップデートの確認およびアップデートの適用を行います。

- インフォメーション

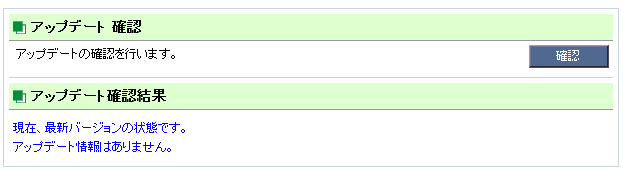
  操作に関する概要を表示します。

- アップデート 確認

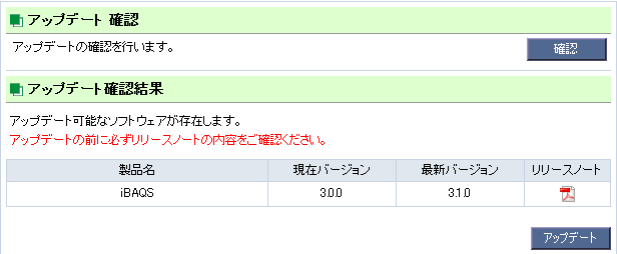
  確認ボタンをクリックすると、アップデートサーバへ接続し、アップデートの確認を行います。確認の結果はアップデート確認結果に表示します。アップデート確認では弊社のアップデートサーバへ http による通信を行います。iBAQS をインターネットと直接通信できる場所に設置するかサーバ設定のプロキシサーバを設定してください。

- アップデート確認結果

  アップデートがない場合には「現在、最新バージョンの状態です。アップデート情報はありません。」と表示します。



アップデートがある場合には「アップデート可能なソフトウェアが存在します。」と表示します。リリースノートのアイコン　をクリックしてリリースノートを確認した上で運用時間以外にアップデートをクリックしてください。アップデートが完了すると自動的に再起動を行います。アップデートは回線状況により時間がかかる場合があります。ブラウザの戻るボタン等で画面を移動すると正常にアップデート処理が行われませんので再起動が行われるまでお待ちください。



- オフラインアップデート

インターネットに接続できない環境でご利用になっている場合には別途オフライン用アップデートファイルを提供しております。ご希望の方は iBAQS 製品サイトをご覧ください。
※オフラインでのご利用はパターンファイルが更新できないため推奨いたしません。

管理

ハードウェア状態.....119
通信確認.....121
ログアウト.....122

ハードウェア状態

ハードウェア状態ではサーバの CPU 使用率、メモリ使用率、ディスク使用率を表示します。画面を表示した際の瞬間値となりますので、詳細な状態遷移は SNMP マネージャから取得してください。

- インフォメーション

  操作に関する概要を表示します。

- 状況

項目	説明	
CPU	CPU の使用率を表示します。	
メモリ	メモリの使用率を表示します。	
	used	プログラム用メモリを表示します。free が不足している場合には buffers や cached からメモリを確保します。
	buffers	バッファ用メモリを表示します。
	cached	キャッシュ用メモリを表示します。
	free	空きメモリを表示します。0%に近くなってもスワップの使用率が増えていなければ特に問題はありません。
スワップ	スワップの使用率を表示します。	

項目	説明	
ディスク	ハードディスクの使用率を表示します。	
	ローカル	ローカルディスクを表示します。デバッグログ、ローカルバックアップ、冗長化対象外の設定情報を格納します
	ミラー	ミラーディスクを表示します。冗長構成時にピアサーバと同期します。冗長化対象の設定内容を格納します。スタントアロン時も利用しています。セカンダリ時には表示しません。

通信確認

通信確認ではネットワーク確認用として ping、traceroute、nslookup を使用できます。疎通確認に ping、traceroute、名前解決確認に nslookup を使用してください。

- インフォメーション

  操作に関する概要を表示します。

- 実行条件

  実行するコマンドおよびパラメータを設定し、実行をクリックします。

項目	パラメータ値	説明
ping	IPv4 アドレス または FQDN	指定したパラメータ値宛に ping を 4 回行います。FQDN を指定する場合には DNS サーバが正しく設定されていることをご確認ください。
traceroute		指定したパラメータ値宛に traceroute を行います。最大 30 ホップまで表示します。FQDN を指定する場合には DNS サーバが正しく設定されていることをご確認ください。
nslookup		指定したパラメータ値の名前解決を行います。

ログアウト

ログアウトをクリックするとログアウトを行います。再度設定を行う場合にはログインボタンをクリックしてください。

セカンダリ

セカンダリ 124
セカンダリ トップ 124
セカンダリ サービス状態 126

セカンダリ

iBAQS では冗長構成時のスタンバイ状態にあるサーバをセカンダリ機と称します。セカンダリ機で利用できるメニューはトップ、サービス状態、サーバ設定、冗長化設定、ライセンス設定、外部連携、管理者設定、ハードウェア状態、通信確認、オンラインマニュアル、ログアウトです。セカンダリ機のトップ、サービス状態はセカンダリ　トップ、セカンダリ　サービス状態を参照してください。それ以外はスタンドアロン/プライマリ機と同じです。

セカンダリ　トップ

セカンダリトップでは各種サマリー情報が表示されます。
各項目に用意されているリンクのアイコンをクリックすることで詳細を確認できます。

- インフォメーション

  インフォメーションにはシステム全体の異常有無を表示します。

- システム状況

<table>
<tr><th>項目名</th><th colspan="3"></th></tr>
<tr><td>ライセンス有効期限</td><td colspan="3">現在登録されているライセンスの有効期限を確認できます。
有効期限が切れるとアップデート等が利用できなくなります。</td></tr>
<tr><td></td><td>状態</td><td>詳細</td><td>意味</td></tr>
<tr><td></td><td>正常</td><td>YYYY/MM/DD</td><td>有効期限まで 31 日以上ある状態</td></tr>
<tr><td></td><td>警告</td><td>YYYY/MM/DD
（期限切れまであと x 日）</td><td>有効期限まで 30 日以内の状態</td></tr>
<tr><td></td><td rowspan="2">異常</td><td>YYYY/MM/DD
（期限切れ）</td><td>有効期限切れの状態</td></tr>
<tr><td></td><td>未取得</td><td>有効期限を取得していない状態</td></tr>
<tr><td>冗長化運転</td><td colspan="3">冗長構成のステータスを確認できます。
異常の場合には正常に動作するプライマリ機と冗長構成を組みなおしてください。</td></tr>
<tr><td></td><td>状態</td><td>詳細</td><td>意味</td></tr>
<tr><td></td><td rowspan="2">正常</td><td>通常運転中です</td><td>設定通りの冗長構成で動作している状態</td></tr>
<tr><td></td><td>切替運転中です</td><td>設定とは逆に冗長構成で動作している状態</td></tr>
<tr><td></td><td>異常</td><td>異常が発生しています</td><td>ピアサーバとの接続に問題がある状態</td></tr>
<tr><td>ミラーディスク</td><td colspan="3">ミラーディスクの状態を確認できます。
強制同期中は再起動、シャットダウンを伴う操作は抑制されます。
状態が異常の場合、単独で起動してもプライマリで動作できません。
ピアサーバを準備し、ピアサーバと強制同期を完了させてください。
ピアサーバと強制同期が完了できない場合にはミラーディスクの物理的な破損の可能性があります。</td></tr>
<tr><td></td><td>状態</td><td>詳細</td><td>意味</td></tr>
<tr><td></td><td rowspan="2">正常</td><td>通常同期中です</td><td>正常にミラーリングを行っている状態</td></tr>
<tr><td></td><td>強制同期中(NN.N%)</td><td>通常同期に加え、差分同期を行っている状態</td></tr>
<tr><td></td><td>異常</td><td>-</td><td>ミラーディスクが論理的に破損している状態</td></tr>
</table>

<table>
<tr><th>項目名</th><th></th></tr>
<tr><td>サービス状態</td><td>iBAQS で利用しているサービス停止の有無を表示します。
異常が発生している場合にはサービス状態画面で停止しているサービスの起動を試みてください。
冗長構成で認証や AVS 確認に必須のサービスが停止している場合にはフェイルオーバーが発生します。
<table>
<tr><th>状態</th><th>詳細</th><th>意味</th></tr>
<tr><td>正常</td><td>正常動作中です</td><td>全てのサービスが正常に動作している状態</td></tr>
<tr><td>異常</td><td>一部停止中です</td><td>1 つ以上のサービスが停止している状態</td></tr>
</table>
</td></tr>
</table>

セカンダリ　サービス状態

セカンダリ　サービス状態では iBAQS の動作に必要なサービスの稼働状況を確認できます。何らかの理由でサービスが停止してしまった場合には起動ボタンにより起動を試みることができます。

- インフォメーション

  インフォメーションにはサービス全体の異常有無が表示されます。

- サービス状態

  サービスの稼働状況を状態に正常 、異常 で表示します。異常 のサービスは起動に表示される起動ボタンで起動できます。

項目名	
NTP	iBAQS の時刻を上位の ntp サーバに同期します。
同期サービス	ミラーディスクを提供します。ピアサーバと接続してミラーディスクの内容を常時同期します。
冗長監視サービス	ピアサーバの死活監視を行い、異常検出時にはプライマリ機へ状態を変更します。
UPS 制御サービス（UPS 連携時）	UPS と通信を行い、UPS が商用電源の異常を検出するとシャットダウンを行います。
SNMP（SNMP 連携時）	SNMP エージェントとして動作し、各種情報を SNMP マネージャに提供します。

その他

スイッチの設定. 129
困ったときは. 135

スイッチの設定

- CentreCOM 8300/8400 シリーズ

  - 通信制限の設定

    ハードウェアパケットフィルターを使用して通信制限を行います。
    事前に iBAQS への通信を許可するための設定が必要です。
    ネットワーク機器設定のフィルタ番号を使用して MAC ベースで制御を行います。
    指定可能なフィルタ番号は 1 から 14 までです。

    ```
    ADD SWITCH L3FILTER MATCH=MACSADDR
    ADD SWITCH L3FILTER MATCH=MACDADDR
    ADD SWITCH L3FILTER=[フィルタ番号+1] ENTRY MACDADDR=[IBAQS の MAC アドレス] ACTION=NODROP
    ADD SWITCH L3FILTER=[フィルタ番号+1] ENTRY MACDADDR=FF:FF:FF:FF:FF:FF ACTION=NODROP
    ADD SWITCH L3FILTER MATCH=DIPADDR DCLASS=HOST
    ADD SWITCH L3FILTER=[フィルタ番号+2] ENTRY DIPADDR=[IBAQS の IP アドレス] ACTION=NODROP
    ADD SWITCH L3FILTER=[フィルタ番号+2] ENTRY DIPADDR=255.255.255.255 ACTION=NODROP
    ```

  - 認証の設定（MAC ベース認証の場合）

    ```
    SET IP LOCAL=1 IPADDRESS=[IP アドレス]
    ADD RADIUS SERVER=[IBAQS の IP アドレス] SECRET=[共有パスワード] PORT=1812 ACCPORT=1813 LOCAL=1
    ENABLE PORTAUTH=MACBASED
    ENABLE PORTAUTH=MACBASED PORT=[ポート番号]
    ```

  - 認証の設定（IEEE 802.1X 認証の場合）

    ```
    SET IP LOCAL=1 IPADDRESS=[IP アドレス]
    ADD RADIUS SERVER=[IBAQS の IP アドレス] SECRET=[共有パスワード] PORT=1812 ACCPORT=1813 LOCAL=1
    ENABLE PORTAUTH=8021X
    ENABLE PORTAUTH=8021X PORT=[ポート番号] TYPE=AUTHENTICATOR
    ```

- CentreCOM 8600/8700 シリーズ

  - 通信制限の設定

    ハードウェアパケットフィルターを使用して通信制限を行います。
    事前に iBAQS への通信を許可するための設定が必要です。
    ネットワーク機器設定のフィルタ番号を使用して IP ベースで制御を行います。
    指定可能なフィルタ番号は 1 から 14 までです。

    ```
    ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST
    ADD SWITCH L3FILTER MATCH=DIPADDR DCLASS=HOST
    ADD SWITCH L3FILTER=[フィルタ番号+1] ENTRY DIPADDR=[IBAQS の IP アドレス] ACTION=NODROP
    ADD SWITCH L3FILTER=[フィルタ番号+1] ENTRY DIPADDR=255.255.255.255 ACTION=NODROP
    ```

  - 認証の設定（MAC ベース認証の場合）

    ```
    SET IP LOCAL=1 IPADDRESS=[IP アドレス]
    ADD RADIUS SERVER=[IBAQS の IP アドレス] SECRET=[共有パスワード] PORT=1812 ACCPORT=1813 LOCAL=1
    ENABLE PORTAUTH=MACBASED
    ENABLE PORTAUTH=MACBASED PORT=[ポート番号]
    ```

  - 認証の設定（IEEE 802.1X 認証の場合）

    ```
    SET IP LOCAL=1 IPADDRESS=[IP アドレス]
    ADD RADIUS SERVER=[IBAQS の IP アドレス] SECRET=[共有パスワード] PORT=1812 ACCPORT=1813 LOCAL=1
    ENABLE PORTAUTH=8021X
    ENABLE PORTAUTH=8021X PORT=[ポート番号] TYPE=AUTHENTICATOR
    ```

- CentreCOM 9400 シリーズ

  - 通信制限の設定

    ハードウェアパケットフィルターを使用して通信制限を行います。
    事前に iBAQS への通信を許可するための設定が必要です。
    ハードウェアパケットフィルターを使用して通信制限を行います。
    事前に iBAQS への通信を許可するための設定が必要です。
    ネットワーク機器設定のフィルタ番号を使用して MAC ベースで制御を行います。
    指定可能なフィルタ番号は 1 から 255 までです。
    フィルタ番号は ACL のエントリーID として使用します。
    クラシファイア番号は 9000 番から自動採番します。9000 番以上のクラシファイア番号は他のハードウェアパケットフィルターで使用しないでください。

    ```
    CREATE CLASSIFIER=8000 MACDADDR=[iBAQS の MAC アドレス]
    CREATE CLASSIFIER=8001 MACDADDR=FF:FF:FF:FF:FF:FF
    CREATE CLASSIFIER=8002 IPSADDR=[iBAQS の IP アドレス]
    CREATE CLASSIFIER=8003 IPSADDR=255.255.255.255
    CREATE ACL=0 ACTION=PERMIT CLASSIFIERLIST=8000-8003 PORTLIST=ALL
    ```

    ※ハードウェアパケットフィルターのエンハンスモードを利用する場合には必ずフィルタ番号を iBAQS への通信を許可するエントリーID よりも大きな値にしてください。

  - 認証の設定（MAC ベース認証の場合）

    ```
    SET IP LOCAL INTERFACE=[vlan-if]
    ADD RADIUSSERVER SERVER=[iBAQS の IP アドレス] ORDER=1 PORT=1812 ACCPORT=1813 SECRET=[共有パスワード]
    ENABLE PORTAUTH
    SET PORTAUTH=MACBASED PORT=[ポート番号] TYPE=AUTHENTICATOR REAUTHENABLED=DISABLED MODE=MULTI
    ```

    ※vlan-if にはネットワーク機器の IP アドレスを持つ VLAN-name か VLAN-id を設定します。

➢ 認証の設定（IEEE 802.1X 認証の場合）

```
SET IP LOCAL INTERFACE=[vlan-if]
ADD RADIUSSERVER SERVER=[iBAQS の IP アドレス] ORDER=1 PORT=1812 ACCPORT=1813 SECRET=[共有パスワード]
ENABLE PORTAUTH
SET PORTAUTH=8021X PORT=[ポート番号] TYPE=AUTHENTICATOR REAUTHENABLED=DISABLED MODE=MULTI
```

※vlan-if にはネットワーク機器の IP アドレスを持つ VLAN-name か VLAN-id を設定します。

- CentreCOM 8900/9900 シリーズ

➢ 通信制限の設定

ハードウェアパケットフィルターを使用して通信制限を行います。
事前に iBAQS への通信を許可するための設定が必要です。
ネットワーク機器設定のフィルタ番号を使用して IP ベースで制御を行います。
指定可能なフィルタ番号は 1 から 14 までです。

```
CREATE CLASSIFIER=8000 MACDADDR=[iBAQS の MAC アドレス]
CREATE CLASSIFIER=8001 MACDADDR=FF-FF-FF-FF-FF-FF
CREATE CLASSIFIER=8002 IPSADDR=[iBAQS の IP アドレス]
CREATE CLASSIFIER=8003 IPSADDR=255.255.255.255
ADD SWITCH HWFILTER CLASSIFIER=8000 ACTION=FORWARD
ADD SWITCH HWFILTER CLASSIFIER=8001 ACTION=FORWARD
ADD SWITCH HWFILTER CLASSIFIER=8002 ACTION=FORWARD
ADD SWITCH HWFILTER CLASSIFIER=8003 ACTION=FORWARD
```

➢ 認証の設定（MAC ベース認証の場合）

```
SET IP LOCAL=1 IPADDRESS=[IP アドレス]
ADD RADIUS SERVER=[IBAQS の IP アドレス] SECRET=[共有パスワード] PORT=1812 ACCPORT=1813 LOCAL=1
ENABLE PORTAUTH=MACBASED
ENABLE PORTAUTH=MACBASED PORT=[ポート番号] MODE=MULTI
```

➢ 認証の設定（IEEE 802.1X 認証の場合）

```
SET IP LOCAL=1 IPADDRESS=[IP アドレス]
ADD RADIUS SERVER=[IBAQS の IP アドレス] SECRET=[共有パスワード] PORT=1812 ACCPORT=1813 LOCAL=1
ENABLE PORTAUTH=8021X
ENABLE PORTAUTH=8021X PORT=[ポート番号] TYPE=AUTHENTICATOR MODE=MULTI
```

- X210/x200/x510/x600/x610/x900 シリーズ/SwitchBlade x908

➢ 通信制限の設定

ハードウェアパケットフィルターを使用して通信制限を行います。
事前に iBAQS への通信を許可するための設定が必要です。
ネットワーク機器設定のフィルタ番号は使用せずに MAC ベースで制御を行います。
アクセスリスト番号は 4100 番から自動採番します。4100 番以上のアクセスリスト番号は他のアクセスリストで使用しないでください。

```
access-list 3000 permit ip any [iBAQS の IP アドレス]/32
access-list 3001 permit ip any 255.255.255.255/32
access-list 4000 permit any [iBAQS の MAC アドレス] 0000.0000.0000
access-list 4001 permit any ffff.ffff.ffff 0000.0000.0000
interface [全てのポート番号]（※x610/x600/x510/x200/x210 シリーズのみ）
ip access-group 3000
ip access-group 3001
mac access-group 4000
mac access-group 4001
```

[⚠ご注意]
x610/x600/x510/x200/x210 シリーズでリンクアグリゲーションや VCS を使用している場合、アクセス制限の設定、解除に時間を要する場合があります。ご了承ください。
x610/x600/x510/x200/x210 シリーズでスタティックチャネル(リンクアグリゲーション)を使用している場合、アクセスリストはスタティックチャネルを構成する物理ポートではなく、スタティックチャネルインターフェースに対して設定してください。

- 認証の設定（MAC ベース認証の場合）

```
ip radius source-interface [IP アドレスまたは IFNAME]
radius-server host [iBAQS の IP アドレス] key [共有パスワード]
aaa authentication auth-mac default group radius
interface [ポート番号]
auth-mac enable
auth host-mode multi-supplicant
```

※IP アドレスまたは IFNAME にはネットワーク機器の IP アドレスまたはネットワーク機器の IP アドレスを持つインターフェース名を設定します。

- 認証の設定（IEEE 802.1X 認証の場合）

```
ip radius source-interface [IP アドレスまたは IFNAME]
radius-server host [iBAQS の IP アドレス] key [共有パスワード]
aaa authentication dot1x default group radius
interface [ポート番号]
dot1x port-control auto
auth host-mode multi-supplicant
```

※IP アドレスまたは IFNAME にはネットワーク機器の IP アドレスまたはネットワーク機器の IP アドレスを持つインターフェース名を設定します。

[⚠ご注意]
x610/x600/x510/x200/x210 シリーズでスタティックチャネル(リンクアグリゲーション)を使用している場合、認証設定はスタティックチャネルを構成する物理ポートではなく、スタティックチャネルインターフェースに対して設定してください。
なお、LACP ポートでは認証を行うことができません。

困ったときは

iBAQS の使用中にトラブルが発生したときは、お問い合わせの前に、もう一度以下の点をお確かめください。

症状	原因	処置
ライセンス登録が行えない	ライセンスキーの入力に誤りがある	0（ゼロ）、O（オー）や1（イチ）、I（アイ）等の違いをご確認ください
ライセンス有効期限が取得できない	弊社のアップデートサーバへhttp通信ができない	デフォルトゲートウェイやプロキシの設定が誤っていないかご確認ください
パターンファイルを更新できない	エフセキュア社のアップデートサーバへhttp通信ができない	デフォルトゲートウェイやプロキシの設定が誤っていないかご確認ください
ネットワーク機器から認証が行えない	ネットワークの疎通ができていない	通信確認の「ping」を用いて接続の可否を確認してください
	ネットワーク機器設定が誤っている	ネットワーク機器設定の IP アドレスや共有パスワードを確認してください
ネットワーク機器の制御が行えない	ネットワークの疎通ができていない	通信確認の「ping」を用いて接続の可否を確認してください
	ネットワーク機器設定が誤っている	ネットワーク機器設定のログイン ID、パスワードを確認してください
	ネットワーク機器に iBAQS への通信許可設定が行われていない	設定例を参考にネットワーク機器に設定を行ってください
検疫クライアントが通信できない	ネットワーク機器に iBAQS への通信許可設定が行われていない	設定例を参考にネットワーク機器に設定を行ってください
	エフセキュア社のアンチウイルス製品を正しく導入していない	iBAQS を管理サーバとしてエフセキュア社のアンチウイルス製品を導入してください

症状	原因	処置
冗長構成でプライマリ機がすぐにシャットダウンしてしまう	接続確認 IP アドレスが ping に応答しない	ping に応答する機器を設置するか接続確認 IP アドレスを変更してください
冗長構成でうまく同期できない	セカンダリ設定機のミラーディスクが優先ディスクになっている	セカンダリ機、プライマリ機の順に起動してください ※プライマリ機の設定情報はセカンダリ機の設定情報で上書きされますのでご注意ください
冗長構成のサーバを単独で起動するとプライマリにならない	強制同期中にピアサーバとの接続が切れてしまった	ピアサーバが起動している状態で障害機を起動してください

ホームページのご案内

iBAQS ホームページでは、最新ソフトウェア情報、よくあるお問い合わせなどを提供しています。本製品を最適にご利用いただくために、定期的にご覧いただくことをおすすめします。

http://www.ib-sol.co.jp/

製品に関するご質問は...

本製品のご質問は下記サポートセンターまでお問い合わせください。

サポートセンター

アイビーソリューション株式会社
〒918-8152 福井県福井市今市町 66-20-2 ホクコンビル 4F
TEL：0776-38-6373　　FAX：0776-38-5341
URL　http://www.ib-sol.co.jp
e-mail：support.ibaqs@ib-sol.co.jp
iBAQS 担当係まで
〈受付時間〉
9:00 ～12:00、13:00 ～ 17:00　月～金（祝・祭日を除く）